PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00, 12/14, H04L 9/00 — A1

(11) International Publication Number: WO 99/03031

(43) International Publication Date: 21 January 1999 (21.01.99)

(21) International Application Number: PCT/SG98/00053

(22) International Filing Date: 3 July 1998 (03.07.98)

(30) Priority Data:
9702398-0 7 July 1997 (07.07.97) SG

(71)(72) Applicants and Inventors: LOW, Huan, Khing [SG/SG]; Blk. 60 Dakota Crescent #06-233, Singapore 390060 (SG). YEO, Chwee, Seng [SG/SG]; Blk. 60 Dakota Crescent #06-233, Singapore 390060 (SG).

(74) Agent: LAWRENCE Y. D. HO & ASSOCIATES; Thongsia Building, 30 Bideford Road #07-01, Singapore 229922 (SG).

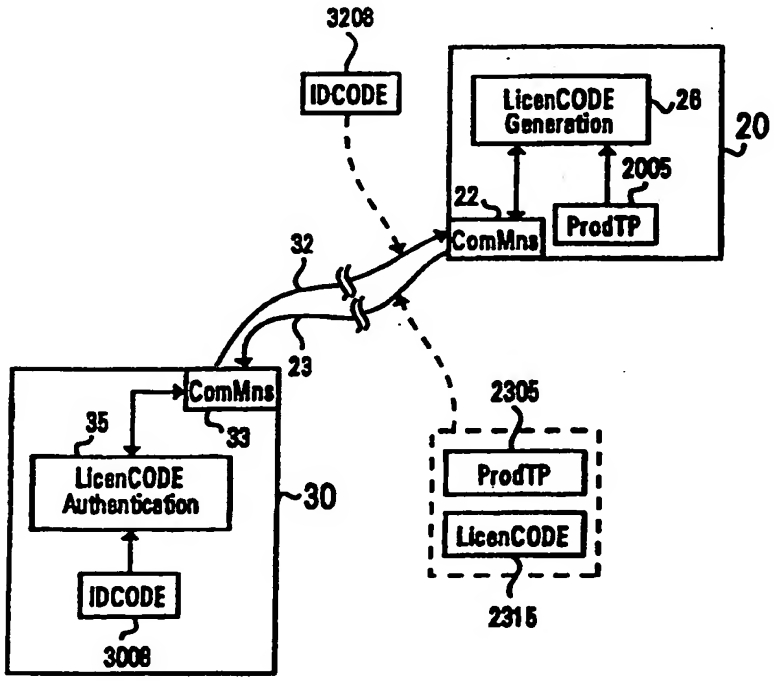
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: A METHOD AND SYSTEM FOR PROTECTING INTELLECTUAL PROPERTY PRODUCTS DISTRIBUTED IN MASS MARKET

(57) Abstract

The present invention is a method and system universally applicable to minimize unauthorized use of intellectual property products distributed to mass market. Identification codes (ID) are assigned to individual intellectual property product and the means of using such product (User Means). Process to minimise unauthorized use of such product includes: firstly, means of selling or distributing such product (Dealer Means) to generate check code from ID of such product stored in said Dealer Means and user supplied ID of User Means. Secondly, Dealer Means supplies such check code to such product placed in said User Means to execute check code authentication by verifying such check code with the code generated from ID of such product and ID of said User Means before allowing use of such product on said User Means to proceed. Alternatively, such check code is generated by User Means from ID of said User Means and ID of such product supplied by individual portable tamper-proof data storage device e.g. plastic card embedded with magnetic storage strip or integrated circuit, such data storage device being distributed together with such product to said User Means. Objectives of the present invention are achieved by embedding essential data and modalities required to execute such check code generation and check code authentication processes into at least one tamper-proof data storage device.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

A METHOD AND SYSTEM FOR PROTECTING INTELLECTUAL PROPERTY PRODUCTS DISTRIBUTED IN MASS MARKET

FIELD OF THE INVENTION

The present invention relates to an authentication process executable during the process of installing or using intellectual property products to prevent unauthorised use and distribution of such products which are recorded on portable means like magnetic or optical or integrated circuit media for distribution to mass market or transmitting such products through mass distribution channel means to users. In particular, the present invention relates to a process of customising intellectual property products with individual authorised user, and to individual predetermined means of using or receiving such products or to both the user and the means at the point of selling or distributing such products or installing such products onto said means.

BACKGROUND OF THE INVENTION

Intellectual property products for mass market are generally recorded on portable storage media for distribution to users in the form of computer software stored in diskette or optical disc or even integrated circuit board, audio and video signal recorded in cassette or optical disk etc. Some of such products are also distributed through mass distribution channel means to the users e.g. software distributed through Internet, audio and video products broadcasted to receivers etc.

Protection schemes to deter piracy or unauthorised use of such products usually cause users inconvenience and may discourage otherwise legitimate purchasers. As a result, owners and producers of intellectual property products either risk piracy by foregoing any form of copy protection or rely on low price business strategy, fast product obsolescence and legal cost remedies approach.

Prior art method of protecting intellectual property products from piracy or unauthorised use include software approach or combination of software approach with hardware solution. The software approach ranges from using password to adopting proprietary encryption and decryption techniques. Available are other techniques such as restrictive duplication procedures and public-key encryption.

Techniques of combining software approach with hardware solution are well illustrated by U.S. Patent No.4,453,074 issued to Weinstein which teaches the use of an encrypted password referenced to the personal characteristics of a "smart-card" possessor. The password is encrypted with a non-secret reference text and stored on the smart-card. When the smart-card possessor presents the smart-card and enters the password on a terminal for accessing a system, the terminal decrypts the embedded password to match with the entered password for allowing the card possessor to gain access to the system while the non-secret reference text is available to the system for identifying the smart-card possessor. Another prior art disclosed by U.S. Patent No.5,343,524 uses a hardware security device within a microprocessor for interacting with a host computer such that protected software may not be operated unless the security device is in place.

European published patent application No.0302710 issued to Karp discloses a technique for authorizing use of diskette software contents on authorized computer by providing a unique identification (ID) placed with a computer which the software on a diskette is to be used. This ID is accessible to the user of the computer. The software vendor provides a source ID on the diskette. The computer ID is used with the source ID to produce an encoded check word, using any available encryption. The check word is then placed onto the distributed diskettes together with the said software. At the time of utilising the software, a verification process is executed by using computer ID and source ID and check word to verify that the software is being used on the same computer on which the diskette was produced. This method requires vendor to store check word together with the software in the distributed diskette making it impractical for mass market because the vendors of products at the time of placing said products on diskettes do not know details of user and his computer.

In general, prior art methods of preventing unauthorised access to computer software distributed to predetermined users do not address unauthorized access after such software are recorded on portable media or after such software are installed onto means of using such software. Moreover, others suggest adding hardware devices to computer system to protect computer software; this approach is not suitable for mass market as these devices are dedicated to individual intellectual property product and are vulnerable to duplication and end users are required to be skilled in the art to some extent. None of the prior art solves the problem of controlling use of intellectual property products stored on portable media and distributed in mass market as owners and producers of such products do not know the users and means of using such products before and after creating such products on portable media for distribution in mass market.

OBJECTIVE OF THE INVENTION

The present invention has an objective of providing a method and system universally applicable to minimise unauthorized use of intellectual property products.

The present invention has another objective of providing a method and system universally applicable to minimise unauthorized use of intellectual property products stored on magnetic media, optical disc or other forms of data storage means.

The present invention has yet another objective of providing a method and system universally applicable to minimise unauthorized use or receipt of intellectual property products transmitted through mass distribution channel means like cable or wireless transmission channel.

SUMMARY OF THE INVENTION

The present invention is a method and system universally applicable to minimise unauthorized use of intellectual property products distributed to mass market. Identification codes (ID) are assigned to individual intellectual property product and the means of using such product (User Means). Process to minimise unauthorized use of such product includes: firstly, means of selling or distributing such product (Dealer Means) to generate check code from ID of such product stored in said Dealer Means and user supplied ID of User Means. Secondly, Dealer Means supplies such check code to such product placed in said User Means to execute check code authentication by verifying such check code with the code generated from ID of such product

and ID of said User Means before allowing use of such product on said User Means to proceed. Alternatively, such check code is generated by User Means from ID of said User Means and ID of such product supplied by individual portable tamper-proof data storage device e.g. plastic card embedded with magnetic storage strip or integrated circuit, such data storage device being distributed together with such product to said User Means.

Objectives of the present invention are achieved by embedding essential data and modalities required to execute such check code generation and check code authentication processes into at least one tamper-proof data storage device.

BRIEF DESCRIPTION OF THE DRAWING

FIGURE 1 illustrates data communication between Dealer Means and User Means for verification of user identity in executing electronic commerce through mass distribution channel means.

FIGURE 1A illustrates the details of User Means generating transaction code for executing electronic commerce through mass distribution channel means.

FIGURE 1B illustrates the details of Dealer Means authenticating transaction code for executing electronic commerce through mass distribution channel means.

FIGURE 2 illustrates the operation of Dealer Means generating LicenCODE to make individual intellectual property product dedicated to individual User Means of using such product and such User Means executing LicenCODE

authentication to install such product for subsequent use on said User Means.

FIGURE 2A illustrates the interaction between Dealer Means and two User Means for changing User Means of using intellectual property product.

FIGURE 3 illustrates User Means in operation of making the fixed tamper-proof data storage device UMIDmeans and the portable tamper-proof data storage device UMIDcard uniquely dedicated to each other as a Match-pair.

FIGURE 3A illustrates the operation of confirming Match-pair condition or unique dedication relationship between fixed tamper-proof data storage device UMIDmeans and portable tamper-proof data storage device UMIDcard in order to enable subsequent installation and application operations of intellectual property products.

FIGURE 4 illustrates the operation of preparing intellectual property product for limited use on User Means after receiving such product through mass distribution channel means, wherein creation of usage control counter for such product in the portable tamper-proof data storage device UMIDcard being described.

FIGURE 4A illustrates the process of controlled usage of installed product on user means where usage control counter having various values in portable tamper-proof data storage device UMIDcard achieves the desired usage control of intellectual property product on User Means.

FIGURE 5 illustrates subsequent to operation in FIGURE 4 the operation of preparing intellectual property product for unlimited use by having Product

tamper-proof data storage device ProdCard to create unlimited use value for usage control counter of such product in portable tamper-proof data storage device UMIDcard.

FIGURE 6 illustrates User Means in operation of disabling use of intellectual property product on the existing User Means in order to enable subsequent installation of such product onto other User Means.

FIGURE 6A illustrates subsequent to operation in FIGURE 6 the operation of installing product onto any User Means.

FIGURE 7 illustrates User Means in operation of creating new fixed tamper-proof data storage device UMIDmeans by duplicating necessary data from the existing portable tamper-proof data storage device UMIDcard to form a new Match-pair for the User Means.

FIGURE 7A illustrates User Means in operation of creating new portable tamper-proof data storage device UMIDcard by duplicating necessary data from the existing fixed tamper-proof data storage device UMIDmeans to form a new Match-pair for the User Means.

FIGURE 7B illustrates User Means in operation of using Product tamper-proof data storage device ProdCard of intellectual property product to enable use of such product on the User Means after creating new fixed tamper-proof data storage device UMIDmeans for such User Means.

FIGURE 7C illustrates User Means in operation of re-enabling limited use of intelligent property product by restoring original value at ProdCPd-limited in

SDOCID: <WO_____9903031A1_I_>

usage control counter for such product in portable tamper-proof data storage device UMIDcard.

FIGURE 8 illustrates data manipulation operation between User Means and Dealer Means of executing pay-per-use transaction through mass distribution channel means for intelligent property product.

FIGURE 8A illustrates the operation of creating usage control counter in portable tamper-proof data storage device UMIDcard to enable limited use of intelligent property product under pay-per-use condition.

FIGURE 9 illustrates the operation of creating usage control counter in portable tamper-proof data storage device UMIDcard to enable limited use of intelligent property product under free product evaluation condition.

FIGURE 10 illustrates Dealer Means in operation of generating LicenCODE for intelligent property product e.g. hardware, audio product and video product etc. in portable tamper-proof data storage device UMIDcard and User Means in operation of executing LicenCODE authentication to enable use of such product.

FIGURE 11 illustrates the Dealer Means in operation of generating LicenCODE for broadcasted intelligent property product in portable tamper-proof data storage device UMIDcard and User Means in operation of executing LicenCODE authentication to enable receipt of such product broadcasted through mass distribution channel means.

FIGURE 12 illustrates the embodiment of applying the present invention to control access to intelligent property product stored in Central Means wherein data manipulation in User Means and Central Means being described.

FIGURE 12A illustrates User Means in operation of generating transaction code to request access right from Central Means for accessing intelligent property product stored in such Central Means.

FIGURE 12B illustrates Central Means in operation of authenticating transaction code for granting User Means the access right.

DETAILED DESCRIPTION OF THE INVENTION

The present invention describes a method and system universally applicable to minimise unauthorized use of intellectual property products (hereinafter called "Product") presented as tangible hardware or intangible signals or intangible signals recorded on any data or signal storage means like magnetic storage means, optical storage means, integrated circuit storage means or the like (hereinafter collectively called "Medium") for distribution through mass distribution channel means to users in mass market. Such mass distribution channel means comprises a combination of at least the telecommunication networks, internet, commercial sales outlets, wireless broadcasting networks for audio and video signal, transportation means, hand delivery or the like (hereinafter collectively called "Channel"). Usually, though not necessarily, said signals take the form of electrical, optical, magnetic or electromagnetic data capable of being stored, transferred, transformed, duplicated, combined, split, and otherwise manipulated.

Notation and Nomenclature

The detailed description with respect to controlling use of Product is presented partially in terms of algorithm and symbolic representation upon data operation and manipulation steps involved. These algorithmic description and representation are the means used by those skilled in the art of data processing to convey most effectively the substance of their work to others skilled in the art.

An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. These steps are those require physical manipulation of physical quantities. Usually, though not necessarily, these quantities take the form of electrical, optical or magnetic signals capable of being stored, transferred, transformed, combined, split, and otherwise manipulated. In this case, the physical quantities are voltage signals which correspond to the information being distributed and processed. It proves convenient at times, principally for reason of common usage, to refer to these voltage signals as bits, bytes, numbers, values, elements, symbols, characters, terms, images or the like. It should be borne in mind, however, all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities.

Furthermore, the manipulations performed are often referred to in terms of such as adding or verifying or comparing, which are commonly associated with the mental operations performed by a human operator. No such capacity of a human operator is necessary, or desirable. In most cases, in any of the operations described herein which form part of the present invention, the operations are machine operations. Useful machines for performing the operations of the present invention include general purpose digital

computers or similar devices such as digital signal processors. In all cases, it should be borne in mind that there is a distinction between the method operation in operating a computer or other apparatus and the method of computation itself. The present invention relates to method steps for preventing unauthorized use of distributed information via storing and manipulation of data within the tamper-proof data storage device, and device being obvious to the one skilled in the art to include software approach like encrypting data and storing such data in hardisk in an unusual way to minimising user access to such data or combination of software approach with hardware solution like manipulating data and storing data within specialised microprocessor which is locked with security key only known to certain known means or people.

The present invention also relates to an apparatus for performing these operations. This apparatus may be specially constructed for the required purpose or it may comprise a general purpose computer as selectively activated or reconfigured by a computer program stored in the computer. The algorithms presented herein are not inherently related to any particular computer or other apparatus. In particular, various general purpose machines may be used with programs written in accordance with the teachings herein, or it may prove more convenient to construct specialized apparatus such as digital signal processor or electronic circuitry to perform the required method steps. The required structure for a variety of these machines would appear from the description given below.

In order to better describe the present invention, some terms and symbols are defined as follows:

individual portable tamper-proof data storage device is assigned to individual Product as "ProdCard", assigned to individual user as "UserCard" and assigned to individual User Means as "UMIDcard"; such device stores essential data and modalities for giving user predetermined access and control window to retrieve or manipulate the data stored in such device and to isolate user from tampering operations of User Means in controlling use of Product such as monitoring, enabling and disabling usage etc.;

individual fixed tamper-proof data storage device "UMIDmeans" is fixed onto each User Means to store data and modalities as well as to interface ProdCard, UserCard and UMIDcard with such User Means;

a plurality of users individually identified by unique user identification code "UserID" and further identified by unique transaction account code "AccountCODE" and optional one or more subsidiary codes "SubCODE"; such codes are stored in Dealer Means, Central Means and respective UserCard for users to execute electronic commerce with said Dealer Means or for users to request access right to retrieve data stored in said Central Means;

a plurality of identification codes CNCODE are individually assigned to represent various considerations, one of which is CityCODE which individually represents each geographical area and group of users;

a plurality of UMIDmeans and UMIDcard are jointly coupled with individual User Means to create unique pair of UMIDmeans and

UMIDcard called "Match-pair" for such User Means through generating and storing an unique identification code "UMID";

a plurality of UMIDcard are individually identified by respective identification code "CardTP";

a plurality of UMIDmeans are individually identified by respective identification code "MeansTP";

a plurality of Products are individually identified by unique product type identification code "ProdTP", such ProdTP is stored in Dealer Means for executing electronic commerce and is also stored in individual ProdCard for dissemination to user in mass market;

a plurality of unique codes "ProdUMID" are the transformed UMID for each Product derived by individual UMIDmeans or UMIDcard from a combination of at least such UMID and ProdTP of individual Product;

a plurality of Product usage counters "ProdCPd" storing quantity of use of individual Product for controlling use of such Product on User Means are individually applicable to respective Product wherein said quantity of use usually, though not necessarily, is presented in any combination of the following forms: frequency of use, time duration, calendar date, volume of data processed or the like;

ProdCPd of a Product having value at "ProdCPd-limited" allows use of such Product subject to predetermined quantity of use;

ProdCPd of a Product having value at "ProdCPd-endless" allows unlimited quantity of use of such Product;

ProdCPd of a Product having value at "ProdCPd-ended" disables use of such Product;

a plurality of User Means are individually identified by identification code IDCODE comprises a combination of at least the identification codes embedded in any part of such User Means, UMID and CNCODE;

a plurality of Product check code "LicenCODE" are individually derived for individual Product from a combination of at least ProdTP of such Product and IDCODE of individual predetermined User Means according to predetermined modalities, so that such LicenCODE is uniquely related to such ProdTP and IDCODE i.e. LicenCODE is a function of ProdTP and IDCODE;

individual User Means comprises means to use Product, Match-pair, and other means and devices coupled with or fixed onto or connected to said means to use Product;

The above terms and symbols should be viewed as the means adopted in the description to conveniently present the details of the present invention to anyone skilled in the art. It should not be viewed as setting limit or scope to the application and claims of the present invention.

In the following description, numerous specific details are set forth such as types of codes used in encryption process and data manipulation steps, etc.

in order to provide a thorough understanding of the present invention. It will be obvious to one skilled in the art that the present invention may be practised without adopting the same details. In other instances, well-known steps such as those involved with encryption and decryption of data are not shown in order not to obscure and restrict implementation of the present invention.

Furthermore, it should be obvious to one skilled in the art that all processes and operations described in the following embodiments can be executed in various general purpose machines. However, in order to isolate user from intervention for achieving the desired objectives, the present invention preferably requires such processes to be executed by any combination of UserCard, ProdCard, UMIDmeans and UMIDcard.

DETAILED DESCRIPTION OF METHOD

The present invention expressed as a method universally applicable to minimise unauthorized use of Product requires IDCODE of User Means and ProdTP of Product for executing LicenCODE Generation and LicenCODE Authentication in customising individual Product with predetermined User Means, and optionally for predetermined considerations like user identity and geographical area etc. by including CNCODE in said LicenCODE Generation and LicenCODE Authentication, as the way to minimise unauthorized use of such Product. Central to this invention are the pairing of at least two tamper-proof data storage devices to form Match-pair as part of User Means; and establishing the unique relationship between Product and User Means by generating a LicenCODE for such Product. Thereafter, User

Means requires to generate a check code to authenticate such LicenCODE in order to use the Product.

LicenCODE Generation is executed by Dealer Means at the stage of distributing Product to User Means for customising such Product with such User Means, or by User Means at Product Installation stage to enable execution of Product Application on such User Means. LicenCODE Authentication is executed by User Means at Product Installation stage to enable execution of Product Application on such User Means for Product distributed by Dealer/Means, or at Product Application stage to enable activation of the use of such Product on such User Means.

Product Installation refers to the process of creating in, storing into or transferring to User Means the data required to execute Product Application and to disable execution of subsequent Product Installation of such Product on such User Means under certain conditions or on other User Means. Said data comprises, but not limited to, LicenCODE of Product required by execution of LicenCODE Authentication, values stored in ProdCPd of Product required by execution of Product Application to control use of such Product on User Means, and flag or data stored in ProdCard of such Product to disable execution of LicenCODE Generation by other User Means. It should be understood by one skilled in the art that values stored in ProdCPD include parameters, numbers, symbols or the like being individually assigned to invoke respective processes to control use of Product, e.g., disabling use of Product, and allowing indefinite use of Product, and allowing use of Product subject to prefixed quantity of use. Such values of ProdCPd are transferable, changeable, duplicable and restorable under predetermined conditions at the stages of Product Installation and Product Application. Product having successfully completed execution of such Product Installation process on

User Means is hereinafter called `Installed Product', and such User Means hereinafter is called `User Means of Installed Product'.

Product Application refers to controlling use of Product on User Means through execution of predetermined combination of the following processes: LicenCODE Authentication, verification and modification of values of ProdCPd of Product, and confirmation of matching CNCODE in Product with CNCODE in User Means. Controlling use of Product refers to enabling, monitoring, recording, disabling use of Product on User Means or the like. LicenCODE Authentication refers to matching LicenCODE of such Product to check code generated by User Means or such Product from IDCODE of user Means and ProdTP of such Product. Verification of values of ProdCPd refers to User Means comparing each value of ProdCPd of Product with a prefixed value for invoking respective processes to control use of such Product on User Means. Modification of values of ProdCPd of Product refers to User Means changing such values of ProdCPd of Product in conjunction with the proceeding of use of such Product on User Means.

The present invention controls use of Product on any User Means through verification of proper values of ProdCPd of such Product stored in portable and detachable tamper-proof data storage device, thus making such Product dedicated to the user owning such portable data storage device. The present invention also allows use of Product to be restricted to User Means of Installed Product through matching of IDCODE stored in such portable tamper-proof data storage device with IDCODE stored in such User Means or through execution of LicenCODE Authentication on such User Means.

ProdTP, IDCODE and ProdCPd are respectively supplied in the complete form by any one of, or in few parts by a combination of, at least the Dealer Means, User Means, ProdCard, UserCard, Product, Medium and Channel.

Dealer Means executing LicenCODE Generation to generate LicenCODE for a Product requires ProdTP of such Product and optional CNCODE for such Product stored in such Dealer Means and IDCODE supplied by User Means through mass distribution channel means or manually delivered to such Dealer Means in a portable data storage device. The generated LicenCODE is subsequently sent by Dealer Means to User Means through mass distribution channel means or manually delivered to User Means in a portable data storage device. Prior to executing Product Installation, such User Means executes a combination of at least the processes of authenticating Match-pair condition and LicenCODE Authentication which comprises matching said LicenCODE with the check code generated by such User Means from IDCODE of such user Means and ProdTP of such Product. The present invention requires said LicenCODE generated by Dealer Means to be separated from Medium of Product for producing homogeneous Product to distribute to mass market.

User Means executing Product Installation without having Dealer Means to generate and supply LicenCODE is defined to execute a combination of at least the processes of authenticating Match-pair condition and generating LicenCODE of such Product from IDCODE of such User Means and ProdTP of such Product. ProdTP is supplied by ProdCard, or Medium of such Product, or Dealer Means through mass distribution channel means, or Dealer Means through a portable data storage device manually delivered to such User Means. After generating said LicenCODE, such User Means proceeds to

SDOCID: <WO_____9903031A1_I_>

execute Product Installation as explained above without executing LicenCODE Authentication.

The present invention requires data and processes relevant or dedicated to User Means for controlling use of Product being partially or completely stored and executed within a combination of at least the Dealer Means, Product, and one or more tamper-proof data storage device. It is to prevent any unauthorised means and people from tampering with said data and processes.

The present invention customises a tamper-proof data storage device with individual User Means by storing in such device the IDCODE of such User. Further customisation is realised by adjusting the subset of IDCODE.

Most of tamper-proof data storage devices are required to be easily detachable from User Means and portable for easy distribution to mass market, whereas the stored data are essential to Product Installation and Product Application; it is therefore necessary to make provision for replacement of faulty or lost of such devices. The present invention requires the data and processes uniquely or exclusively related to individual User Means being stored in at least two such devices, so that replacement of one such device is executed by duplicating such data from another such device. However, such data duplication process also allows others to duplicate many such devices such that unauthorized use of Product on other User Means is possible. To overcome this problem, the present invention requires to disable duplication of ProdCPd at value of ProdCPd-endless for unlimited quantity of use of Product, to change part or whole of IDCODE of such User Means and such device for such User Means in each execution of such replacement

process; and further requires a Match-pair to execute Product Installation and optionally Product Application.

The present invention refers said Match-pair to as at least one fixed tamper-proof data storage device called "UMIDmeans" permanently fixed onto each User Means e.g. a smart-card driver, and at least one portable tamper-proof data storage device called "UMIDcard" to be coupled with said UMIDmeans e.g. a smart-card. Both UMIDmeans and UMIDcard store the data and modalities necessary for execution of Product Application of Installed Products. As such, one may place said UMIDcard onto any UMIDmeans to use said Installed Products on any User Means if execution of Product Application of such Products requires no Match-pair condition between said UMIDcard and said any UMIDmeans. For each Match-pair, an unique identification code "UMID" is generated and stored together with optional CNCODE assigned for various considerations in both UMIDmeans and UMIDcard. An unique MatchCODE is derived from said UMID and optional CNCODE and stored in said UMIDmeans and UMIDcard. The present invention refers Match-pair condition to as successful execution of two tests, where the first test is to verify UMID and CNCODE stored in UMIDmeans with UMID and CNCODE stored in UMIDcard; and the second test is to execute MatchCODE Authentication which requires generation of a check code from said UMID and CNCODE for authenticating MatchCODE stored in said Match-pair.

DESCRIPTION OF FIRST EMBODIMENT OF THE PRESENT INVENTION

The first embodiment of the present invention describes the process of Dealer Means controlling use of Product distributed through mass distribution channel means.

1. Verification of User Identity for Electronic Commerce Transaction

In detail now and referring to FIGURE 1 it shows data involved in communication between Dealer Means 20 and User Means 30 for verifying user identity in order to execute electronic commerce over mass distribution channels 23 and 32. Upon receiving request (not shown) of executing electronic commerce from User Means 30, a RandomNUM Generator 24 in Dealer Means 20 generates a random number RandomNUM 2313 and transmits via communication means ComMns 22 of Dealer Means through mass distribution channel 23 to User Means 30 and receives via communication means ComMns 33. In response, User Means 30 generates and sends TransactCODE 3204 and order data 3207 to Dealer Means 20 via ComMns 33 through mass distribution channel 32 to Dealer Means 20 via ComMns 22, where TransactCODE 3204 is generated by a TransactCODE Generator 34 (to be explained in FIGURE 1A later) and order data 3207 is the encrypted details of the ordered Product.

FIGURE 1A shows the details of encryption process of a TransactCODE Generator 34 executed by User Means 30. The received RandomNUM 2313 is verified by CHK VALIDITY 341 to confirm validity in accordance to predetermined rules, CODE ENCRYPT 342 then uses the verified RandomNUM 2313 to encrypt user's account codes AccountCODE 3002 and subsidiary codes SubCODE 3003, followed by MERGE ENCRYPT 343 to merge the result with the verified RandomNUM 2313 into TransactCODE 3204. CODE ENCRYPT 342 also uses RandomNUM 2313 to encrypt details of the ordered Product like ProdTP 3005 and other data 3006 of the ordered Product to generate order data 3207. Finally both TransactCODE 3204 and

order data 3207 are sent to Dealer Means 20 as mentioned in FIGURE 1 above.

FIGURE 1B shows details of decryption process executed by Dealer Means 20 to verify user identity. The received TransactCODE 3204 passes through SPLITCODE 251 to filter out RandomNUM 2313 which is then verified by CHK VALIDITY 252 to confirm whether it is the same random number sent previously to User Means 30. COMPARE CODE 254 compares the stored AccountCODE 2002 and SubCODE 2003 with the result of CODE DECRYPT 253 generated by decryption of the remaining part of TransactCODE 3204 using the verified RandomNUM 2313. Path 256 to approve electronic commerce request is activated upon confirmation of user identity through same AccountCODE and SubCODE being detected by COMPARE CODE 254; otherwise, path 257 to reject such electronic commerce request is activated.

2. Dealer Means Distribute Product and Control Use of Product via Mass Distribution Channel Means

FIGURE 2 explains the data manipulation processes within Dealer Means 20 and User Means 30 together with data transmission between Dealer Means 20 and User Means 30 for minimizing unauthorised use of Product distributed by Dealer Means 20 through mass distribution channel means 23. In response to approval notice (not shown) for electronic commerce request received from Dealer Means 20, User Means 30 transmits stored identification codes IDCODE 3008 from ComMns 33 through mass distribution channel 32 via ComMns 22 to Dealer Means 20 as IDCODE 3208. IDCODE 3008 or IDCODE 3208 are the identification codes of the User Means predetermined to use the ordered Product (in this embodiment

User Means 30 is assumed to be such User Means). A LicenCODE Generation 26 in Dealer Means 20 encrypts such IDCODE 3208 and ProdTP 2005 stored in Dealer Means 20 to generate an unique LicenCODE 2315. Dealer Means 20 sends LicenCODE 2315 and ProdTP 2305 of the ordered Product together with the ordered Product (optional, not shown) e.g. computer software, via ComMns 22 through mass distribution channel 23 to User Means 30 via ComMns 33. Thereafter, User Means 30 executes LicenCODE Authentication 35 to compare LicenCODE 2315 with the result generated by encrypting IDCODE 3008 and ProdTP 2305 in order to execute Product Installation to store or create data in User Means 30, where such data is necessary for subsequent use of the ordered Product.

User usually receives the ordered Product distributed through mass distribution channel means earlier than settlement of payment. In order to enable certain fixed quantity of use of such Product prior to settlement of payment, Dealer Means 20 sends value at ProdCPd-limited to store into ProdCPd of ordered Product in User Means 30. Such quantity of use is reduced progressively towards the value of ProdCPd-ended while use of ordered Product is in progress. Such value at ProdCPd-ended will disable use of ordered Product on User Means 30. Thereafter should payment be settled, Dealer Means 20 sends value at ProdCPd-endless to store into ProdCPd of ordered Product in User Means 30 for unlimited quantity of use of ordered Product on User Means 30. As such, it makes provision to disable use of ordered Product should there be default payment.

The process to change User Means for the Installed Product, i.e., the ordered Product having completed execution of Product Installation on such User Means, is explained in FIGURE 2A. Step 931 initiates the request to change User Means 30 to User Means 38, followed by step 932 to execute

LicenCODE Authentication to confirm proper execution of Product Installation for such Product on User Means 30. Step 933 deletes LicenCODE and value at ProdCPd-endless stored in ProdCPd of such Product in User Means 30 and step 934 sends IDCODE 3008 of User Means 30 including ProdTP of such Product to Dealer Means 20. Step 941 in Dealer Means 20 then matches IDCODE 3008 and such ProdTP with the record stored in Dealer Means 20. Upon confirming the matching, step 942 generates and stores RandomNUM followed by step 943 to send such RandomNUM to User Means 30. At step 935, user transfers such RandomNUM from User Means 30 to User Means 38, whereby in step 945 sends such RandomNUM and IDCODE 3808 of User Means 38 to Dealer Means 20 to request in step 944 to generate new LicenCODE for such Product based on IDCODE 3808 and such ProdTP. Thereafter, Dealer Means 20 replaces IDCODE 3008 by IDCODE 3808 in the record to prepare next request of changing User Means 38 to other User Means, and sends such new LicenCODE to User Means 38 to execute Product Installation of ordered Product on User Means 38 by matching such new LicenCODE to the result generated by encrypting IDCODE 3808 and ProdTP of ordered Product in order to store or create in User Means 38 the data necessary for the use of ordered Product on User Means 38.

Process in FIGURE 2A has the first disadvantage in that upon User Means 30 failing to send IDCODE 3008 to Dealer Means 20 to request RandomNUM e.g. due to faulty User Means, re-installation of such Product on other User Means is not feasible. The second disadvantage is the process vulnerability to unauthorized duplication of LicenCODE and ProdCPd-endless (hereinafter "derived codes") for execution of Product Application in more than one User Means. It is possible to duplicate such derived codes elsewhere, then execute process in Fig 2A, such that the deleted drived

codes in User Means 30 is restorable for continuous use of such Product on User Means 30.

DESCRIPTION OF SECOND EMBODIMENT OF THE PRESENT INVENTION

The second embodiment of the present invention describes the processes of adopting Match-pair to control use of Product distributed through mass distribution channel means.

1. Install Match-pair

The present invention describes another embodiment to overcome the disadvantages of the first embodiment by requiring creation of individual UMIDmeans and UMIDcard Match-pair for individual User Means and using individual ProdCard for each Product. All the essential data like IDCODE, ProdTP, LicenCODE, ProdCPd etc. necessary for execution of LicenCODE Authentication, Product Application and other essential processes are stored in UMIDmeans, UMIDcard and ProdCard which are tamper-proof data storage devices and mostly detachable from User Means, it is practically not possible to duplicate said data stored in such devices and failure of User Means will not affect proper execution of such devices on other User Means. Furthermore, there are other advantages that will be explained subsequently in FIGURE 3 to 7C.

IDCODE 3008 of User Means 30 (similar to IDCODE 3808 of User Means 38 or IDCODE of other User Means) mentioned in FIGURE 2A above are generated and stored in UMIDmeans 40 and UMIDcard 50 as shown in FIGURE 3, wherein IDCODE 3008 comprises mainly, but not limited to UMID

and CityCODE. Process 80 in FIGURE 3 describes the creation of a Match-pair of UMIDcard and UMIDmeans for individual User Means. UMIDcard is the portable tamper-proof data storage device which couples and works with UMIDmeans. UMIDmeans is a tamper-proof data storage device permanently coupled to User Means.

Process 80 begins with verification of proper UMIDcard and UMIDmeans (not shown) used in execution of process 80. It is mainly to ensure no UMID is stored in UMIDmeans and UMIDcard. Thereafter, step 801 copies CityCODE 5018 in UMIDcard 50 into UMIDmeans 40 as CityCODE 4018 for making both UMIDmeans 40 and UMIDcard 50 storing the same CityCODE which forms part of IDCODE to relate said User Means to the geographical area and user group specified by CityCODE 5018. Subsequently, step 802 generates a random number UMID for said User Means, and step 803 derives MatchCODE from such UMID, CardTP 5019 of UMIDcard 50, CityCODE 4018 and MeansTP 4020 of UMIDmeans 40 to make such MatchCODE uniquely related to such UMID, CardTP, CityCODE and MeansTP. Finally, step 804 stores such MatchCODE into UMIDmeans 40 as MatchCODE 4014 and UMIDcard 50 as MatchCODE 5014, and step 805 stores such UMID into UMIDmeans 40 as UMID 4009 and UMIDmeans 50 as UMID 5009. UMIDmeans 40 and UMIDcard 50 are thereby created as a Match-pair for such User Means.

In execution of some processes like installing Product onto User Means (to be explained later), it is necessary to confirm whether UMIDmeans and UMIDcard have the same IDCODE and uniquely linked to each other as a Match-pair. Such confirmation is executed in a 2-step test as shown by process 81 in FIGURE 3A. Step 811 executes the first test to confirm whether CityCODE 5018 and UMID 5009 in UMIDcard 50 are the same as CityCODE

4018 and UMID 4009 in UMIDmeans 40 respectively. Step 812 then executes the second test to derive code from CardTP 5019 of UMIDcard 50 and CityCODE 4018, UMID 4009 and MeansTP 4020 in UMIDmeans 40 followed by confirming that such code is the same as MatchCODE 4014 in UMIDmeans 40. Upon successful confirmation of the above 2 tests (hereinafter called "Match-pair Authentication"), UMIDcard 50 and UMIDmeans 40 are confirmed as a Match-pair.

2. Installation for Limited Use of Product Received through Mass Distribution Channel Means Prior to Settlement of Payment

FIGURE 4 explains the Product Installation process 82 of involving Match-pair to enable limited quantity of use of Product prior to settlement of payment. Step 821 begins process 82 by initiating step 822 to execute Match-pair Authentication, failure of step 822 evades process 82 whereas success of step 822 activates step 823 and step 824 to confirm that no LicenCODE of such Product is stored in UMIDmeans 40 and UMIDcard 50 as the way to ensure no prior execution of Product Installation of such Product to avoid duplicated installation of such Product. Process 82 is evaded if such LicenCODE is found in either UMIDmeans 40 or UMIDcard 50, otherwise step 825 LicenCODE Authentication is executed by matching LicenCODE 2315 received from Dealer Means 20 (see FIGURE 2) to check code derived from IDCODE (not shown) stored in UMIDmeans 40 and ProdTP 2305 supplied by Dealer Means 20 as the way to confirm LicenCODE 2315 is properly generated for the Match-pair of UMIDmeans 40 and UMIDcard 50. Failure in step 825 evades process 82; otherwise, step 826 stores LicenCODE 2315 in UMIDcard 50 and stores value at ProdCPd-limited supplied by such Product in ProdCPd of such Product in UMIDcard 50 to enable limited quantity of use of such Product (to be explained in FIGURE 4A

later). Finally, step 827 stores LicenCODE 2315 in UMIDmeans 40 and stores value at ProdCPd-ended supplied by such Product in ProdCPd of such Product in UMIDmeans 40 as the record of execution of such Product Installation process in order to disable future installation of such Product for free evaluation (to be explained in FIGURE 9 of fourth embodiment).

Process 83 in FIGURE 4A explains the execution of controlled use of Installed Product on User Means. UMIDcard 50 having value stored in ProdCPd of such Product is coupled with UMIDmeans (not shown) of any User Means to execute process 83 to use such Product on such User Means. Upon initiation of request to use such Product (not shown), for the case that use of such Product is permitted only on the User Means of Installed Product, step 831 executes Match-pair and LicenCODE Authentication to confirm UMIDcard 50 and UMIDmeans (not shown) being a Match-pair and such Product being the Installed Product of said Match-pair. Subsequently, step 832 is invoked to check whether value of ProdCPd-endless is stored in ProdCPd of such Product in UMIDcard 50. Upon confirmation of finding such ProdCPd-endless, step 833 is called to proceed with use of such Product; otherwise, step 834 is invoked to check whether value at ProdCPd-ended is stored in ProdCPd of such Product in UMIDcard 50. Upon confirmation of finding such ProdCPd-ended, step 835 is called to evade use of such Product. If not, the use of such Product proceeds in steps 837. While use of such Product is in progress, step 836 constantly modifies value of ProdCPd of such Product in UMIDcard 50 towards the value at ProdCPd-ended. Use of such Product is disabled upon value of ProdCPd in UMIDcard 50 reaching ProdCPd-ended. Thus, execution of Product Installation of such Product allows predetermined quantity of use of such Product specified by the value at ProdCPd-limited stored in ProdCPd of such Product in UMIDcard 50.

It is obvious to the one skilled in art that by ignoring step 831 to allow Product Application to be executed on any User Means, such Product is restricted only to the user using UMIDcard 50; otherwise, execution of step 831 will make use of such Product dedicated to predetermined User Means associated with such Match-pair of UMIDmeans and UMIDcard 50.

3. Installation for Unlimited Use of Product Received through Mass Distribution Channel Means After Settlement of Payment

As explained in FIGURE 4A, user may use Installed Product indefinitely on any User Means if value at ProdCPd-endless is stored in ProdCPd of such Product in UMIDcard, while Match-pair and LicenCODE Authentication is ignored. Process 84 in FIGURE 5 explains the creation of such ProdCPd-endless in ProdCPd of such Product in UMIDcard. After settlement of payment, ProdCard 60 of such Product is dispatched to such User Means to be coupled with UMIDmeans 40. Step 841 of process 84 requests step 842 to verify proper codes being stored in ProdCard 60 for executing process 84 and CityCODE (not shown) stored in ProdCard 60 being the same as CityCODE (not shown) stored in UMIDmeans 40 to confirm such ProdCard conforming to same geographical area and user group of Match-pair. Thereafter, step 843 LicenCODE Authentication is executed to match LicenCODE stored in UMIDmeans 40 with check code derived from IDCODE stored in UMIDmeans 40 and ProdTP (not shown) supplied by ProdCard 60 as the way to ensure such Product having been installed properly by process 82. Failure in step 843 evades process 84; otherwise, step 844 is activated to store ProdUMID into ProdCard 60 for customising ProdCard 60 with such Match-pair of UMIDmeans 40 and UMIDcard 50. Step 845 stores into ProdCPd 5021 in UMIDcard 50 the value at ProdCPd-limited for predetermined quantity of use of such Product and stores into ProdCPd 4021

in UMIDmeans 40 the value at ProdCPd-limited for restoring such limited quantity of use of such Product (to be explained in FIGURE 7C later). Finally, step 846 transfers ProdCPd-endless 6024, if there is, from ProdCard 60 to overwrite such ProdCPd-limited in ProdCPd 5021 of such Product in UMIDcard 50 and then erases ProdCPd-endless 6024 in ProdCard 60. Value at ProdCPd-endless stored in ProdCPd of such Product in UMIDcard 50 will not be changed in conjunction with use of such Product.

4. Change Match-pair of Installed Products

Match-pair for individual Installed Product is changeable through process 85 in FIGURE 6. ProdCard 60 of such Product is coupled with UMIDmeans 40 to commence process 85 by having step 851 to request step 852 to verify whether ProdUMID (not shown) stored in ProdCard 60 is the same as the ProdUMID (not shown) stored in UMIDmeans 40, and step 853 LicenCODE Authentication further ensures such Product is the Installed Product of the Match-pair consisting of UMIDmeans 40 and UMIDcard 50. Thereafter, step 854 clears ProdUMID in ProdCard 60 and step 855 transfers ProdCPD-endless in ProdCPd 5021 of such Product in UMIDcard 50 back to ProdCard 60 as ProdCPd-endless 6024, thus ProdCard 60 is available to execute Product Installation of such Product on any Match-pair associated with any User Means. Finally step 856 erases LicenCODE 4015, LicenCODE 5015, ProdCPd 4021 and ProdCPd 5021 of said Product stored respectively in UMIDmeans 40 and UMIDcard 50 to disable use of such Product on such Match-pair of UMIDmeans 40 and UMIDcard 50.

Product Installation of such Product on any other Match-pair consisting of UMIDmeans 48 and UMIDcard 58 is executed by process 86 in FIGURE 6A, using ProdCard 60 without involving Dealer Means 20 to re-generate

LicenCODE. Upon coupling ProdCard 60 with UMIDmeans 48, step 861 initiates step 862 to verify whether ProdCard 60 is suitable to execute process 86 on such Match-pair by confirming that no ProdUMID is stored in ProdCard 60 and that the same CityCODE (not shown) of such Match-pair is stored in Prodcard 60 to ensure compatibility in geographical area and user group. Thereafter, LicenCODE Generation in step 863 generates LicenCODE (not shown) from ProdTP supplied by ProdCard 60, and IDCODE by UMIDmeans 48, respectively. Step 864 then stores into ProdCard 60 the ProdUMID supplied by UMIDmeans 48 to customise ProdCard 60 with such Match-pair of UMIDmeans 48 and UMIDcard 58, and step 865 stores such LicenCODE as LicenCODE 4815 and LicenCODE 5815 and stores the value at ProdCPd-limited in ProdCPd 4821 and ProdCPd 5821 for predetermined quantity of use of such Product. Finally, step 866 transfers ProdCPd-endless 6024, if there is, from ProdCard 60 to overwrite such ProdCPd-limited in ProdCPd 5821 in UMIDcard 58, followed by erasing ProdCPd-endless 6024 in ProdCard 60.

5. Replacing Faulty or Missing UMIDmeans or UMIDcard of a Match-pair

Data relevant or dedicated to User Means and essential for executing Product Installation and Product Application are stored in both UMIDmeans and UMIDcard of each match-pair. It is necessary to duplicate such data in new device for creating replacement of faulty or lost device. The present invention refers such device to as UMIDmeans and UMIDcard and such new device to as such device yet to be used to form a Match-pair. Meanwhile provision must also be in place to make the abandoned device (i.e. the faulty or lost UMIDmeans or UMIDcard) irrelevant to the new Match-pair which consists of an existing device and a new device.

The present invention requires replacement of one device at a time. The abandoned device is made irrelevant to the new Match-pair through the process of generating new UMID for the new Match-pair. The present invention requires to use ProdCard of Installed Product to generate new LicenCODE of such Product in such new Match-pair for such new UMID, and further requires to customise ProdCard with the new Match-pair by storing new ProdUMID derived from such new UMID in such ProdCard to prevent execution of Product Installation on other Match-pair. Finally, it is necessary to create records of all Installed Product in new Match-pair to prevent duplicated execution of Product Installation of such Product on new Match-pair for free use (to be explained in FIGURE 9 later).

FIGURE 7 shows process 87 in details to create new Match-pair consisting of new UMIDmeans 44 and existing UMIDcard 50. After replacing existing UMIDmeans 40 by new UMIDmeans 44 and coupling existing UMIDcard 50 with UMIDmeans 44, step 871 copies CityCODE 5018 in UMIDcard 50 into UMIDmeans 44 as CityCODE 4418 to make both UMIDmeans 44 and UMIDcard 50 applicable to same geographical area and user group specified by CityCODE 5018. Next, step 872 generates new UMID followed by step 873 to derive new MatchCODE from such new UMID, together with CardTP 5019 in UMIDcard 50 and CityCODE 4418 and MeansTP 4420 in UMIDmeans 44 respectively. Thereafter, step 874 stores such new MatchCODE in UMIDmeans 44 as MatchCODE 4414 and replaces existing MatchCODE in UMIDcard 50 as MatchCODE 5014. Subsequently, step 875 erases LicenCODE 5015 of all Installed Products, and step 876 retains ProdCPd-endless 5024 of all Installed Products in UMIDcard 50 followed by creating ProdCPd-ended in ProdCPD 5021 for all Installed Products and coping such ProdCPd-ended from ProdCPd 5021 to UMIDmeans 44 as ProdCPd 4421. Finally, step 877 copies existing Old UMID 5010 in UMIDcard

50 to UMIDmeans 44 as Old UMID 4410 (the purpose of retaining existing Old UMID will be explained in FIGURE 7B), and step 878 stores such new UMID in UMIDcard 50 as New UMID 5011 and in UMIDmeans 44 as New UMID 4411. At this stage, execution of process 87 to create new Match-pair consisting of new UMIDmeans 44 and existing UMIDcard 50 is completed and UMID of such new Match-pair is such new UMID.

FIGURE 7A shows a process 88 in details to create new Match-pair consisting of existing UMIDmeans 40 and new UMIDcard 55. After coupling new UMIDcard 55 with existing UMIDmeans 40, step 881 ensures CityCODE 5518 in UMIDcard 55 is the same as CityCODE 4018 in UMIDmeans 40. Next, step 882 generates new UMID followed by step 883 to derive new MatchCODE from such new UMID together with CardTP 5519 in UMIDcard 55, and CityCODE 4018 and MeansTP 4020 in UMIDmeans 40. Next, step 884 stores such new MatchCODE in MatchCODE 5514 and replaces existing MatchCODE in MatchCODE 4014 by such new MatchCODE. Subsequently, step 885 erases LicenCODE 4015 of all Installed Products, while step 886 creates values at ProdCPd-ended in ProdCPD 4021 for all Installed Products and copies such ProdCPd-ended from ProdCPd 4021 to ProdCPd 5521 in UMIDcard 55. Finally, step 887 copies existing Old UMID 4010 in UMIDmeans 40 to UMIDcard 55 as Old UMID 5510, and step 888 stores such new UMID in UMIDmeans 40 as New UMID 4011 and in UMIDcard 55 as New UMID 5511. At this stage, execution of process 88 to create new Match-pair consisting of new UMIDcard 55 and existing UMIDmeans 40 is completed and UMID of such new Match-pair is such new UMID. It is clear to the one skilled in the art that only the abandoned UMIDcard 50 (not shown) stores ProdCPd at values of ProdCPd-endless for all Installed Products. It also follows that ProdCPd-endless is not retained in process 88 and prevents new UMIDcard 55 to store any ProdCPd-endless for the Installed Product. As

such, it prevents creation of ProdCPd-endless for Installed Product in multiple UMIDcards.

Process 89 in FIGURE 7B explains the details of a process to re-enable Product Application of Installed Products after replacing UMIDmeans 40 by new UMIDmeans 44. Execution of process 89 is required for each Installed Product by using respective ProdCard to create new LicenCODE of such Product from new UMID, thereafter customising such ProdCard with new Match-pair. When one couples ProdCard 60 of individual Installed Product and existing UMIDcard 50 with new UMIDmeans 44 concurrently or separately, step 891 initiates step 892 to verify that ProdCard 60 is dedicated to old UMID by testing the existence of old ProdUMID in ProdCard 60. If the testing fails, process 89 is evaded; otherwise, step 893 derives LicenCODE for such Product from new ProdUMID and other subset of IDCODE stored in UMIDmeans 44. Subsequently, step 894 replaces old ProdUMID (not shown) in ProdCard 60 by new ProdUMID to customise ProdCard 60 with new Match-pair, and step 895 stores such LicenCODE of such Product in LicenCODE 5015 and LicenCODE 4415 followed by replacing existing value of ProdCPd 5021 and ProdCPd 4421 of such Product by ProdCPd-limited. Finally, step 896 transfers the retained ProdCPd-endless 5024 of such Product to replace existing ProdCPd-limited which is created by step 895 in ProdCPd 5021.

Process 89 is also applicable to replacement of UMIDcard 50 by new UMIDcard 55 except that step 896 is not required due to non existence of ProdCPd-endless in ProdCPd in new UMIDcard 55.

As explained in FIGURE 4A, UMIDcard having value at ProdCPd-endless stored in ProdCPd of Installed Product allows unlimited quantity of use of

such Product on the Match-pair of such Product or on any Match-pair if use of such Product does not require a Match-pair. Value at ProdCPd-limited stored in ProdCPd of such Product only allows predetermined quantity of use of such Product as specified by such ProdCPd-limited. It is because such ProdCPd-limited will be modified towards ProdCPd-ended while use of such Product is in progress. Such ProdCPd storing no value at ProdCPd-endless is caused by replacement of UMIDcard as explained in 7A and 7B above.

As explained in FIGURE 7 and 7A, UMID of a Match-pair is changed after replacement of UMIDmeans or UMIDcard. Such change in UMID firstly disables use of Installed Products on any User Means if one uses the abandoned UMIDcard to execute Product Application requiring a Match-pair. Secondly, such change in UMID also limits use of Installed Products on any User Means to the quantity of use of such Product specified by ProdCPd-limited of such Product in the abandoned UMIDcard, if one uses such abandoned UMIDcard to execute Product Application not requiring a Match-pair. After value of ProdCPd having reached ProdCPd-ended, such abandoned UMIDcard for such Product is useless because restoration of such ProdCPd-limited in such abandoned UMIDcard can only be executed by the Match-pair on which Product Installation of such Product is executed.

The present invention allows restoration of ProdCPd-limited in ProdCPd of Installed Product in UMIDcard of a Match-pair for achieving practically unlimited quantity of use of such Product on any User Means, if one uses such UMIDcard to execute Product Application not requiring a Match-pair. Process 90 in FIGURE 7C explains such restoration process in details. By coupling UMIDcard 55 with UMIDmeans 40, step 901 initiates step 902 to test whether UMIDmeans 40 and UMIDcard 55 are the Match-pair. Failure to step 902 calls step 903 to evade process 90; otherwise, success of step 902

causes steps 904 and 905 to test whether value of ProdCPd 4021 of each Installed Product is greater than the value of ProdCPD 5521 of such Product. This is followed by activating the optional step 906 to execute LicenCODE Authentication of such Product, prior to activating step 907 to replace value of ProdCPd 5521 of such Product by the value at ProdCPd-limited (not shown) stored in ProdCPd 4021 of such Product, if value of ProdCPd 4021 is greater than the value of ProdCPd 5521. Step 908 will complete process 90 for all Installed Products in UMIDcard 55 after executing step 904 to 907 for each of such Installed Products.

DESCRIPTION OF THIRD EMBODIMENT OF THE PRESENT INVENTION

The third embodiment of the present invention requires no involvement of Dealer Means, but requires a Match-pair of UMIDmeans and UMIDcard. Referring to FIGURE 6A again, the present invention requires individual ProdCard 60 for each Product being distributed together with such Product e.g. packaged box software, to users in mass market. Product Installation of such Product on any User Means associated with a Match-pair is handled by process 86 as explained in FIGURE 6A above.

Execution of controlled use of such Installed Product on User Means is handled by process 83 as explained in FIGURE 4A above.

Process 85 in FIGURE 6 as explained above prepares ProdCard 60 for allowing such Installed Product to change User Means associated with another Match-pair.

Process 89 to re-enable Product Application of such Installed Product is already explained in FIGURE 7B above. Execution of process 89 is necessary due to change of UMID caused by replacing UMIDmeans 40 by new UMIDmeans 44 or replacing UMIDcard 50 by new UMIDcard 55,

If a Product has no value of ProdCPd-endless for ProdCPd stored in UMIDcard to allow unlimited quantity of use of such Product on any User Means, as explained in FIGURE 7C above, process 90 is invoked to restore value of ProdCPd-limited into such ProdCPd for achieving practically unlimited quantity of use of such Product on any User Means. One reason of causing such ProdCPd without value of ProdCPd-endless is replacement of UMIDcard.

DESCRIPTION OF FOURTH EMBODIMENT OF THE PRESENT INVENTION

The fourth embodiment of the present invention describes the processes of controlling limited quantity of use of Products sold for occasional use like pay per use, contracted period of use etc. Such Products are mainly distributed through mass distribution channel means or dispatched in Medium. For this embodiment, verification of User Identity for executing electronic commerce is already described in Figure 1, 1A and 1B.

Referring to FIGURE 8, data manipulation and data communication between Dealer Means 20 and User Means 30 is similar to FIGURE 2, except that FIGURE 8 requires UMIDcard 50 to generate and store at least one random number RandomNUM 5013. This random number is required by Dealer Means 20 to generate unique and different LicenCODE for each occasional use request of same Product by the same User Means. UMIDmeans 40 and

UMIDcard 50 are not necessary a Match-pair for selling use of such Product on any User Means. UMIDcard 50 sends RandomNUM 5013 together with IDCODE 5008 through UMIDmeans 40 via communication means ComMns 33 through mass distribution channel (not shown) to Dealer Means 20 as RandomNUM 3213 and IDCODE 3208 respectively. A LicenCODE Generation 26 in Dealer Means 20 then derives LicenCODE of Product from IDCODE 3208, RandomNUM 3213 and ProdTP 2005 of such Product stored in Dealer Means 20 respectively. Finally, Dealer Means 20 sends such LicenCODE as LicenCODE 2315 via communication means ComMns 22 through mass distribution channel 23 and via ComMns 33 to User Means 30. It should be obvious to the one skilled in the art that such random number can also be generated by Dealer Means 20 instead of by UMIDcard 50 for achieving the same purpose of deriving unique and different LicenCODE for each occasional use request.

Subsequently, a process 91 in FIGURE 8A executes Product Installation of such Product when one couples UMIDcard 50 with UMIDmeans 40 to activate step 911 to initiate step 912 to match LicenCODE 2315 with check code derived from ProdTP supplied by such Product (not shown), IDCODE 5008 and RandomNUM 5013 stored in UMIDcard 50 for confirming such Product being dedicated to UMIDcard 50. If not, step 912 evades process 91; otherwise, step 912 proceeds to step 913 to erase RandomNUM 5013 as the way to disable subsequent execution of Product Installation of such Product. Next, step 914 stores the value at ProdCPd-limited supplied by such Product or Dealer Means 20 into ProdCPd 5021 of such Product to enable subsequent execution of Product Application of such Product through UMIDcard 50, whereby such ProdCPd-limited restricts use of such Product by predetermined quantity of use. Finally, the optional step 915 creates value at ProdCPd-ended in ProdCPd 4021 of such Product in UMIDmeans 40 to

disable execution of Product Application of such Product for free evaluation which will be explained in FIGURE 9 later.

DESCRIPTION OF FIFTH EMBODIMENT OF THE PRESENT INVENTION

Commercial practice of allowing free predetermined quantity of use of Product for evaluation is common. The fifth embodiment of the present invention explains process 92 in FIGURE 9 for said purpose, where step 921 initiates step 922 to confirm whether UMIDmeans 40 and UMIDcard 50 are unique Match-pair. If not, step 922 evades process 92; otherwise, steps 923 and 924 ensure no prior free use of such Product on such Match-pair by confirming non existence of ProdCPd 5021 of such Product in UMIDcard 50 and ProdCPd 4021 of such Product in UMIDmeans 40. Finally, step 925 stores value at ProdCPd-limited supplied by such Product or Dealer Means 20 in ProdCPd 5021 of such Product, and step 926 creates record of free use in UMIDmeans 40 by storing value at ProdCPd-ended in ProdCPd 4021 of such Product.

DESCRIPTION OF SIXTH EMBODIMENT OF THE PRESENT INVENTION

The sixth embodiment of the present invention describes the method of controlling use of Product stored in Medium and distributed to user at the point of sales e.g. audio and video Products distributed in cassette or optical disk. Referring to FIGURE 10, user supplies UMIDcard 50 to Dealer Means 20 where a LicenCODE Generation 26 derives LicenCODE of Product 71

from IDCODE 5008 of User Means 30 and ProdTP 2005 of such Product according to encryption modality EncryCODE 2025 of such Product. The IDCODE 5008 is stored in UMIDcard 50 and ProdTP 2005 is stored in Dealer Means 20. Thereafter, such LicenCODE is stored in UMIDcard 50 as LicenCODE 5015.

User couples Product 71 and UMIDcard 50 with User means 30 to initiate use of Product 71 on User Means 30. A LicenCODE Authentication 35 compares LicenCODE 5015 stored in UMIDcard 50 with the check code derived from IDCODE 3008 stored in User Means 30 and ProdTP 7105 supplied by Product 71 according to decryption modality DecryCODE 7126 stored in Product 71. Proper match of LicenCODE 5015 with such check code enables one to use Product 71 on User Means 30. It is understood by the one skilled in the art that using IDCODE 5008 stored in UMIDcard 50 for generating said check code allows one to use such Product on any User Means.

DESCRIPTION OF SEVENTH EMBODIMENT OF THE PRESENT INVENTION

The seventh embodiment of the present invention describes a method of controlling receipt of Product disseminated as broadcasted signal via mass distribution channel means. User supplies UMIDcard 50 to Dealer Means 20. where a LicenCODE Generation 26 derives LicenCODE from IDCODE 5008 stored in UMIDcard 50 and ProdTP 2005 stored in Dealer Means 20. Such LicenCODE is stored in UMIDcard 50 as LicenCODE 5015. Optionally, a CHANGE DecryCODE 27 replaces decryption modality DecryCODE 5026 stored in UMIDcard 50.

User couples UMIDcard 50 with User Means 30 to initiate receipt of such Product by User Means 30. A LicenCODE Authentication 35 compares LicenCODE 5015 stored in UMIDcard 50 with the check code derived from IDCODE 3008 stored in User Means 30 and ProdTP 1305 of Product received from mass distribution channel means according to the decryption modality DecryCODE 5026 stored in UMIDcard 50. A proper match of LicenCODE 5015 with such check code activates RECEIVER CONTROL 37 to receive such Product. It is understood by the one skilled in the art that using IDCODE 5008 stored in UMIDcard 50 for generating said check code allows one to use any User Means to receive such Product.

DESCRIPTION OF EIGHTH EMBODIMENT OF THE PRESENT INVENTION

The eighth embodiment of the present invention describes a method of controlling access to data stored in a Central Means. Referring to FIGURE 12, user couples UserCard 70 with UMIDmeans 40 to request access right, such request (not shown) is sent to a Central Means 10 via ComMns 33 through transmission channel 31 and via ComMns 11 to Central Means 10. Upon receipt of such request, a RandomNUM Generator 14 of the Central Means 10 generates an unique RandomNUM 1313 for such request and sends RandomNUM 1313 via ComMns 11 through transmission channel 13 and via ComMns 33 to User Means 30. Thereafter, a TransactCODE Generator 34 of User Means 30 derives unique TransactCODE 3104 from RandomNUM 1313, UserID 7001 and SubCODE 7003 retrieved from the UserCard 70 and sends TransactCODE 3104 via ComMns 33 through transmission channel 31 and via ComMns 11 to Central Means 10. Upon receipt of TransactCODE 3104, TransactCODE Authentication 15 of Central

Means 10 authenticates TransactCODE 3104 to verify the user's identify before granting user the access right.

FIGURE 12A explains the process of TransactCODE Generator 34 in details. RandomNUM 1313 received from Central Means 10 is firstly verified by CHK VALIDITY 701 according to predetermined rules. A CODE ENCRYPT 702 then generates TransactCODE 3104 by using verified RandomNUM 1313 to encrypt UserID 7001 and SubCODE 7003.

FIGURE 12B explains the process of TransactCODE Authentication 15 in details. Upon receipt of TransactCODE 3104 from User Means 30, a CODE DECRYPT 151 of Central Means 10 uses the stored RandomNUM 1313 to decrypt TransactCODE 3104 into user identity codes and passes such user identity codes to a COMPARE CODE 152 to compare with the stored UserID 1001 and SubCODE 1003. Step 153 acts upon the result of such comparison to activate path 154 on the result of proper match by granting such user the access right or to activate path 155 on the result of mismatch by rejecting access request of such user.

While the present invention has been described particularly with reference to FIGURE 1 to 12B with emphasis on a method and system for protecting intellectual property products distributed in mass market, it should be understood that the figures are for illustration only and should not be taken as a limitation on the invention. In addition, it is clear that the method and system of the present invention have utility in many applications where secure electronic transmission and verification of information are required. It is contemplated that many changes and modifications may be made by one of ordinary skill in the art without departing from the spirit and the scope of the invention as described.

CLAIMS

1. A method for maximising the security of distributing intellectual property products over a channel, said channel having at least one Dealer Means communicating with at least one User Means, said method comprising the steps of:

assigning identification codes ProdTP for each said products and IDCODE for each said User Means respectively;

requiring said Dealer Means to generate a LicenCODE from a first combination of at least said ProdTP and said IDCODE, said User Means further generating a Checkcode from a second combination of at least said ProdTP and said IDCODE; and

controlling the use of said products on any said User Means by executing a third combination of processes for authenticating said LicenCODE with said Checkcode,

whereby embedding at least said ProdTP in a tamper-proof data storage device to be used with any User Means minimises the unauthorised use of said products over said channel.

2. The method for maximising the security of distributing intellectual property products as in claim 1 wherein said LicenCODE is the same as the said Checkcode, said LicenCODE being generated by said Dealer Means.

3. The method for maximising the security of distributing intellectual property products as in claim 1 wherein said LicenCODE is generated by said Dealer Means and said Checkcode is generated by said User Means, said Checkcode further incorporating at least a portion of said LicenCODE.

4. The method for maximising the security of distributing intellectual property products as in claim 1 wherein said first combination is the same as the second combination.

5. The method for maximising the security of distributing intellectual property products as in claim 1 wherein the use of said products on any said User Means comprises the installation of said products on any said User Means.

6. The method for maximising the security of distributing intellectual property products as in claim 1 wherein the use of said products on any said User Means comprises the application of said products on any said User Means.

7. The method for maximising the security of distributing intellectual property products as in claim 1 wherein the use of said products on any said User Means comprises the activation of the use of said products on any said User Means.

8. The method for maximising the security of distributing intellectual property products as in claim 1 wherein said products further comprises at least one product usage counter ProdCPd, the value of ProdCPd permitting

the controlled use of said products and said Dealer Means allowing the regeneration of said LicenCODE in altering the identity of User Means.

9. The method for maximising the security of distributing intellectual property products as in claim 1 wherein said channel comprises a network.

10. A method for maximising the security of distributing intellectual property products as in claim 1 wherein said tamper-proof data storage device comprises a smart card.

11. A method for maximising the security of distributing intellectual property products as in claim 1 wherein the execution of the authentication of said LicenCODE and Checkcode comprises the step of encoding and decoding with a random number RandomNUM.

12. A method for maximising the security of distributing intellectual property products as in claim 1 wherein the authentication of said LicenCODE and Checkcode comprises the step of encoding and decoding with a predetermined code.

13. A method for maximising the security of distributing intellectual property products as in claim 1 wherein the execution of said third combination of processes comprises the processes of authenticating said LicenCODE with said Checkcode and confirming that said product usage counter ProdCPd has the proper value.

14. A method for maximising the security of distributing intellectual property products over a channel, said channel having at least one Dealer

Means communicating with at least one User Means, said method comprising the steps of:

assigning identification codes ProdTP for each said products, and UMID for a matched pair of UMIDmeans and UMIDcard, said matched pair being associated uniquely with each said User Means and for providing backup for said matched pair;

requiring said Dealer Means to generate a LicenCODE from a combination of at least said ProdTP and said UMID respectively;

generating by each said User Means a Checkcode from a combination of said ProdTP and UMID respectively; and

controlling the use of said products on any said User Means by requiring the authentication of said LicenCODE with said Checkcode,

whereby embedding at least said ProdTP, LicenCODE or UMID in said matched pair to be used with predetermined User Means minimises the unauthorised use of said products over said channel.

15. The method for maximising the security of distributing intellectual property products as in claim 14 wherein the use of said products on any said User Means comprises the installation of said products on any said User Means.

16. The method for maximising the security of distributing intellectual property products as in claim 14 wherein the use of said products on any said

User Means comprises the application of said products on any said User Means.

17. The method for maximising the security of distributing intellectual property products as in claim 14 wherein the use of said products on any said User Means comprises the activation of the use of said products on any said User Means.

18. The method for maximising the security of distributing intellectual property products as in claim 14 wherein said UMID is changeable without requiring said Dealer Means to regenerate a LicenCODE, said changed UMID being associated uniquely with a different matched pair for allowing the regeneration of said LicenCODE and Checkcode in altering the identity of said User Means.

19. The method for maximising the security of distributing intellectual property products as in claim 14 wherein UMID is changeable to disable abandoned matched pair or abandoned UMID Means or UMIDcard to prevent unauthorised duplication thereof.

20. The method for maximizing the security of distributing intellectual property products as in claim 14 wherein said channel comprises a wireless boardcasting network for audio and video signals.

21. A method for maximizing the security of distributing intellectual property products as in claim 14 wherein said UMIDcard is a tamper-proof data storage device.

22. A method for maximizing the security of distributing intellectual property products as in claim 14 wherein said UMIDmeans is a tamper-proof data storage device.

23. A method for maximizing the security of distributing intellectual property products as in claim 14 wherein the authentication of said LicenCODE and Checkcode comprises the step of encoding and decoding with a random number RandomNUM.

24. A method for maximizing the security of distributing intellectual property products as in claim 14 wherein the authentication of said LicenCODE and Checkcode comprises the step of encoding and decoding with a predetermined code.

25. A method for maximising the security of distributing intellectual property products in a mass market having at least one User Means and at least one product card ProdCard associated with each said products, said method comprising the steps of:

assigning identification codes ProdTP for each said products and UMID for a matched pair of UMIDmeans and UMIDcard, said matched pair being associated uniquely with each said User Means and for providing backup for said matched pair;

generating by said matched pair a LicenCODE from a combination of ProdTP and UMID respectively, said ProdTP original only from said ProdCard;

generating by said User Means a Checkcode from a combination of said ProdTP and UMID; and

controlling the use of said products on any User Means by requiring the authentication of said LicenCODE and said Checkcode,

whereby embedding UMID, ProdTP or LicenCODE in said matched pair and in said ProdCard respectively minimises unauthorised use of said products distributed in a mass market.

26. A method for maximising the security of distributing intellectual property products in a mass market as in claim 25 wherein said UMID is embedded in said ProdCard for associating said ProdCard with said matched pair.

FIGURE 1A

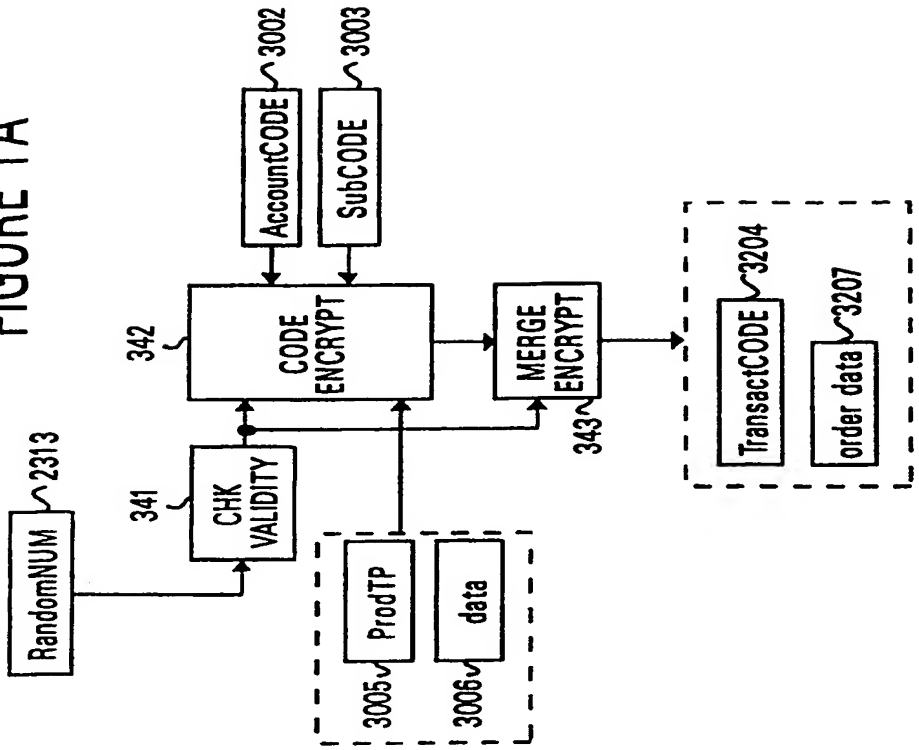
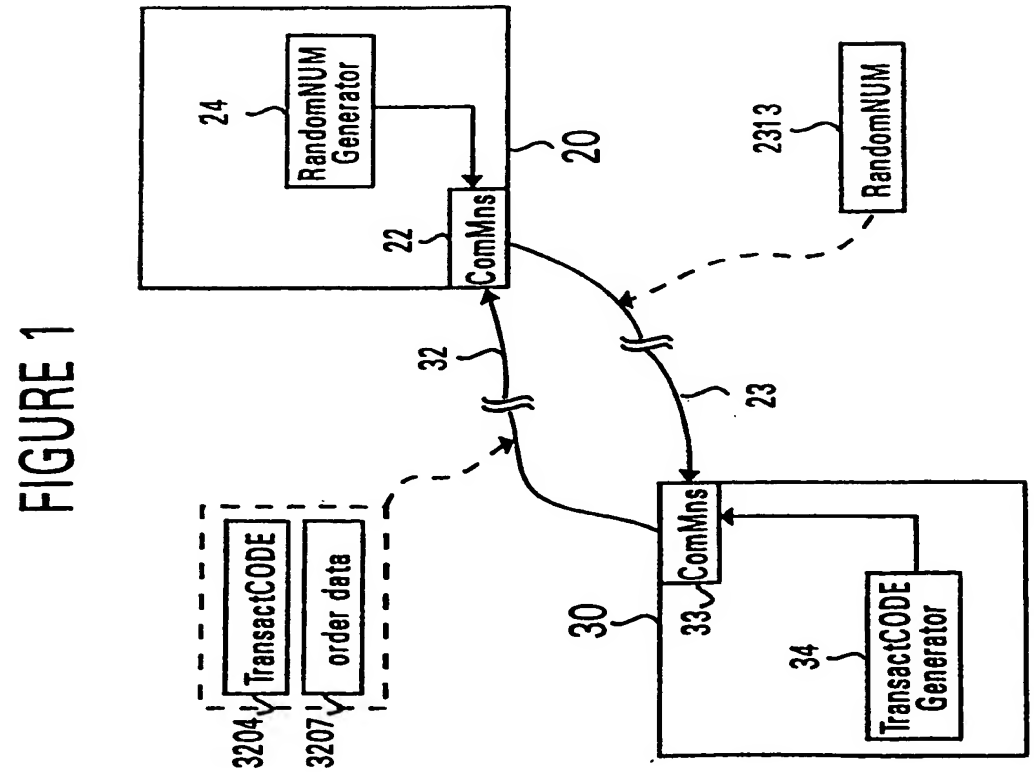


FIGURE 1



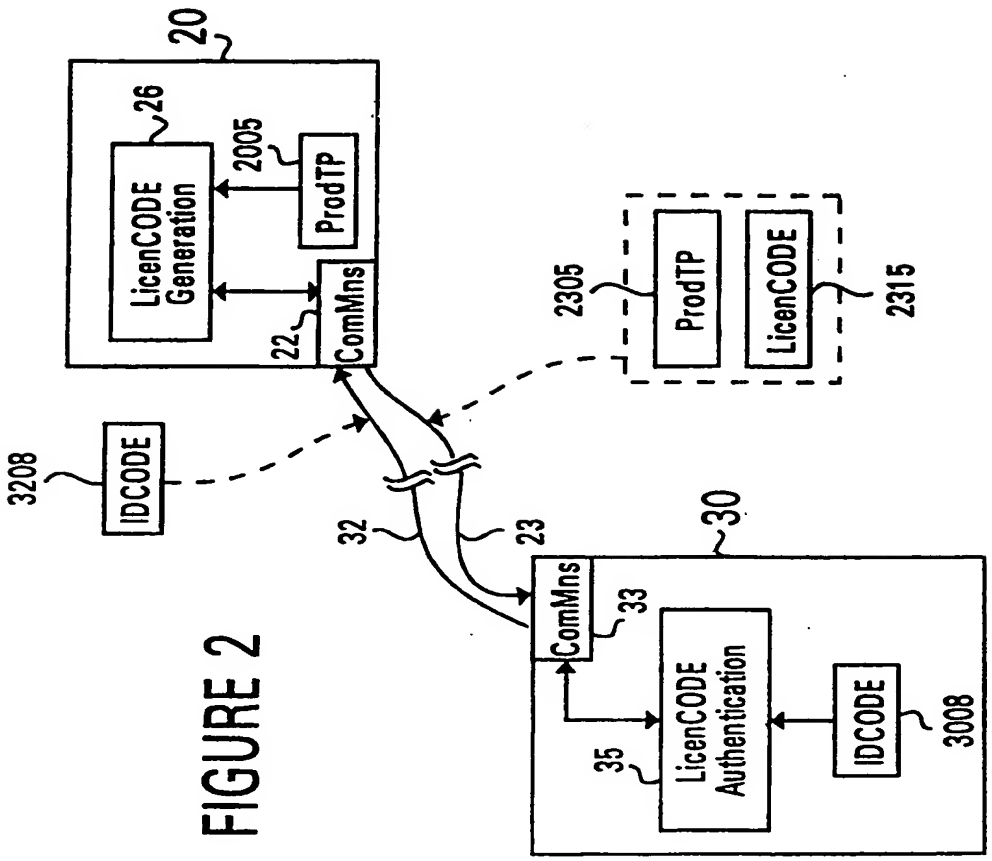


FIGURE 2

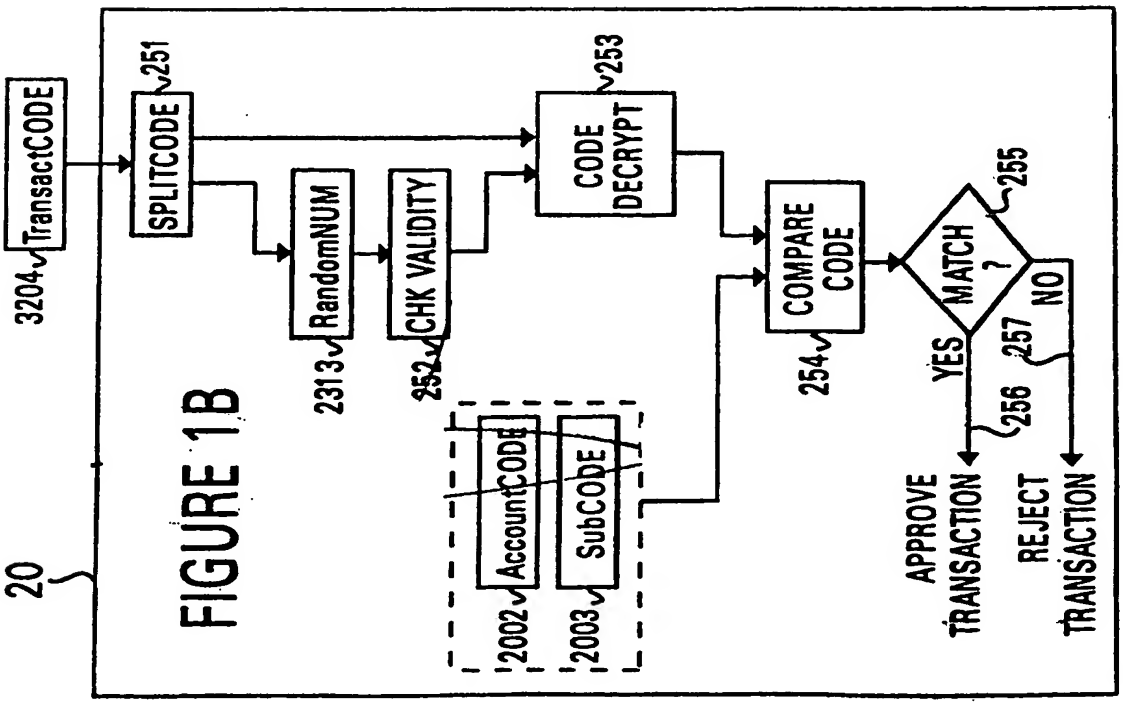


FIGURE 1B

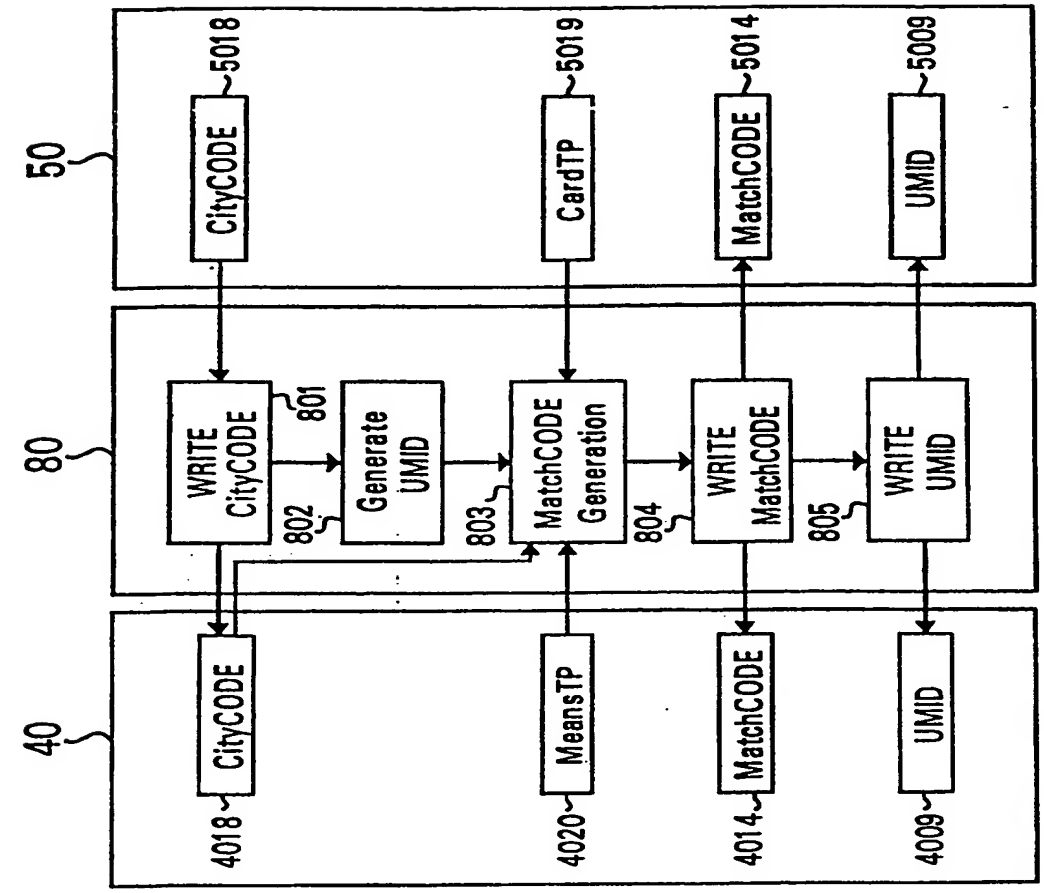


FIGURE 3

FIGURE 2A

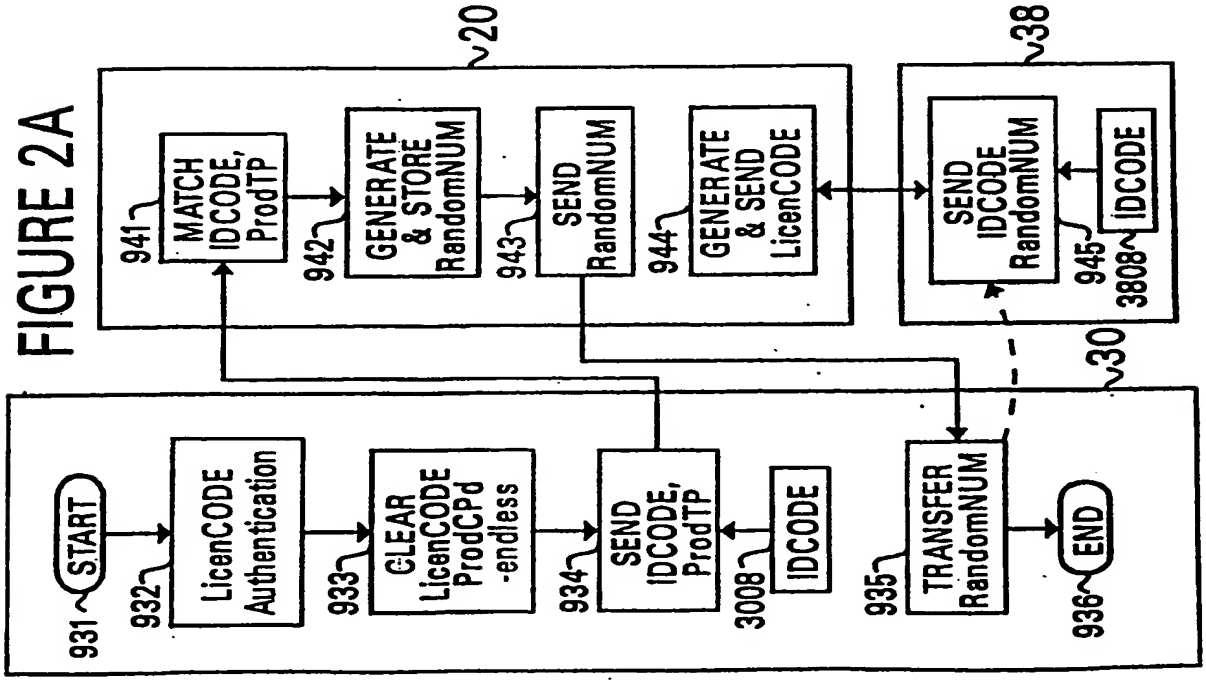
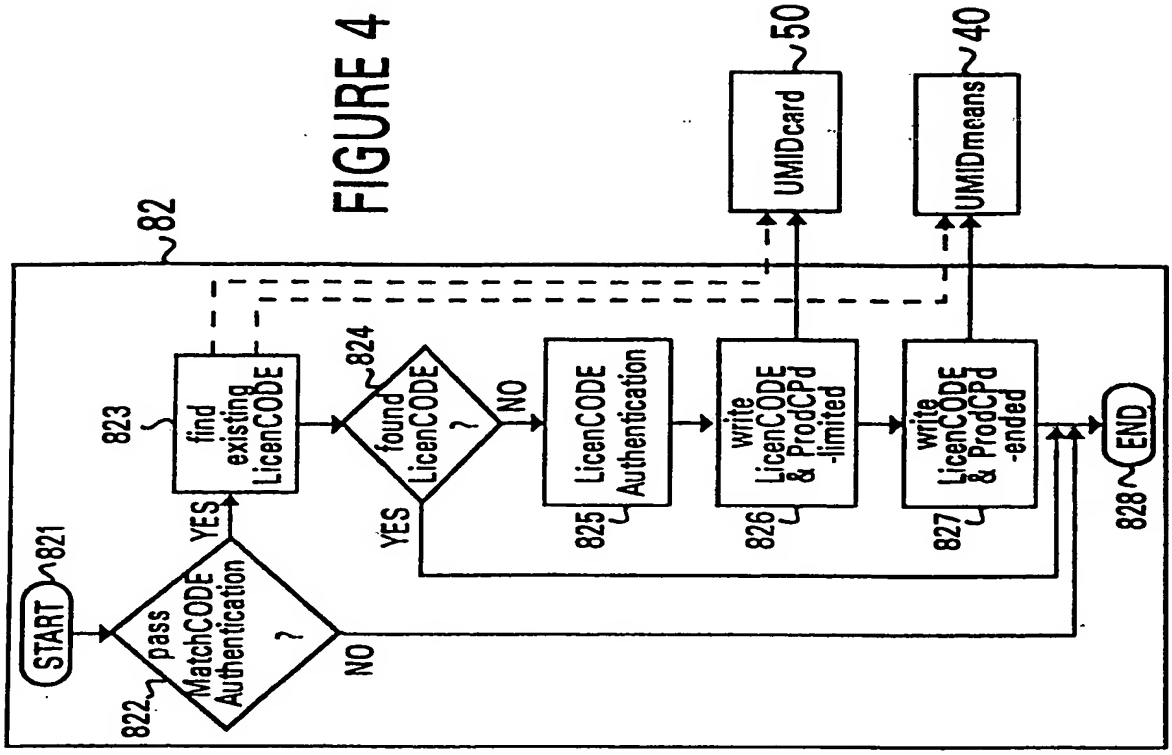


FIGURE 4



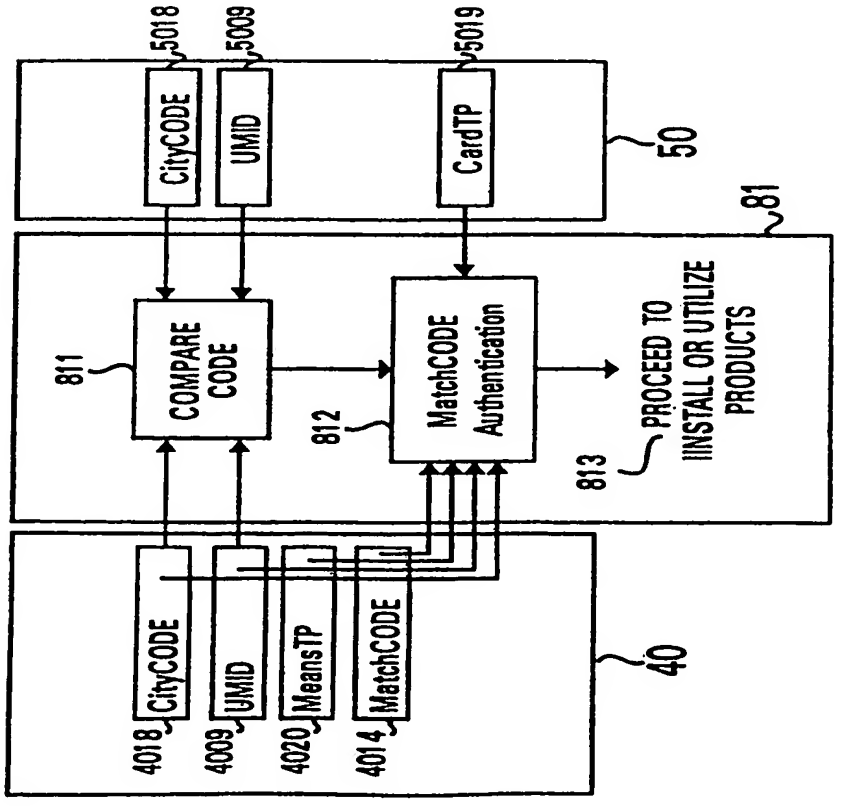


FIGURE 3A

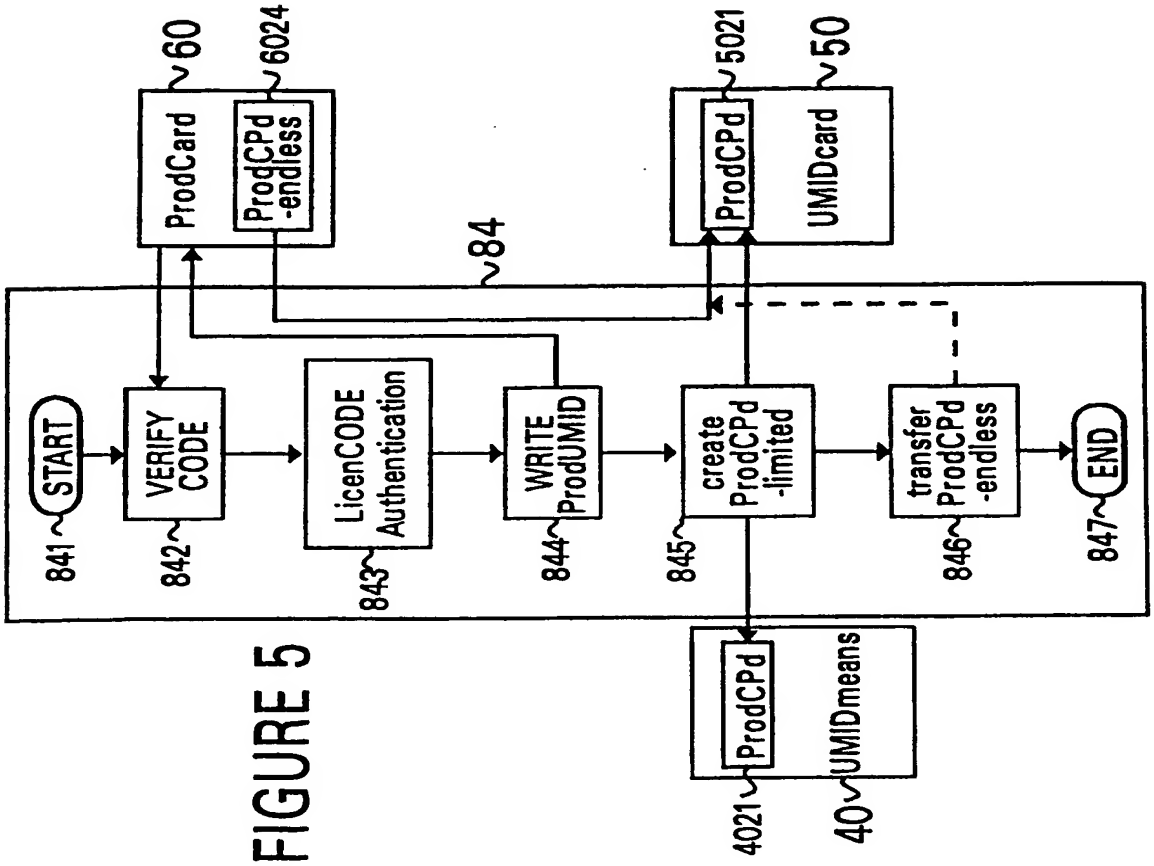


FIGURE 5

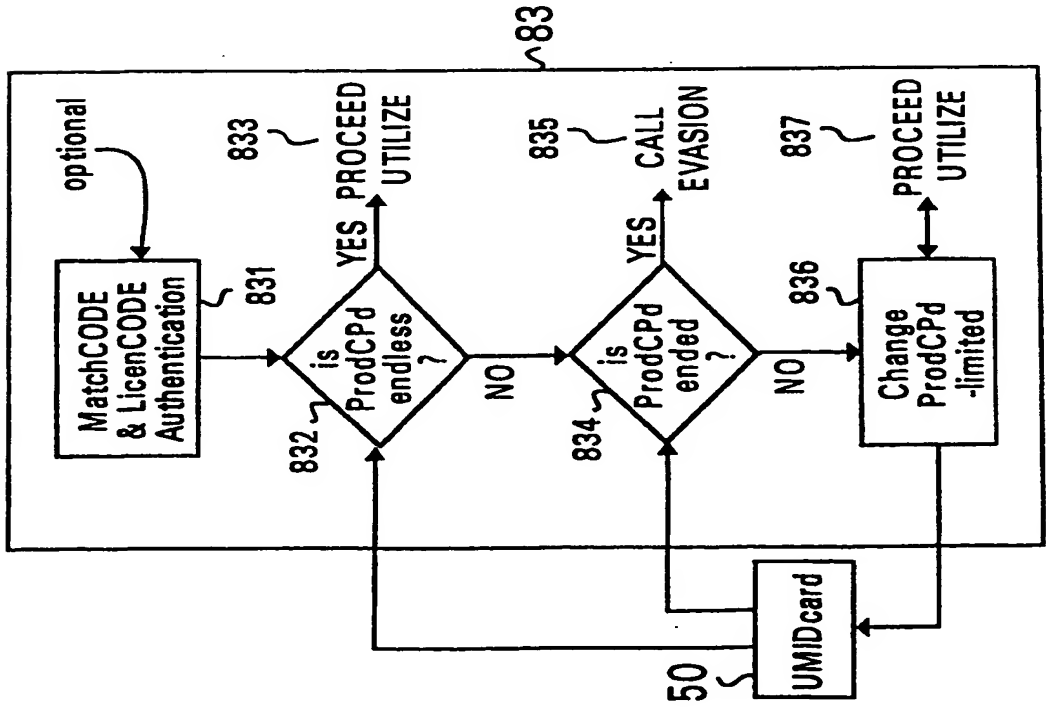


FIGURE 4A

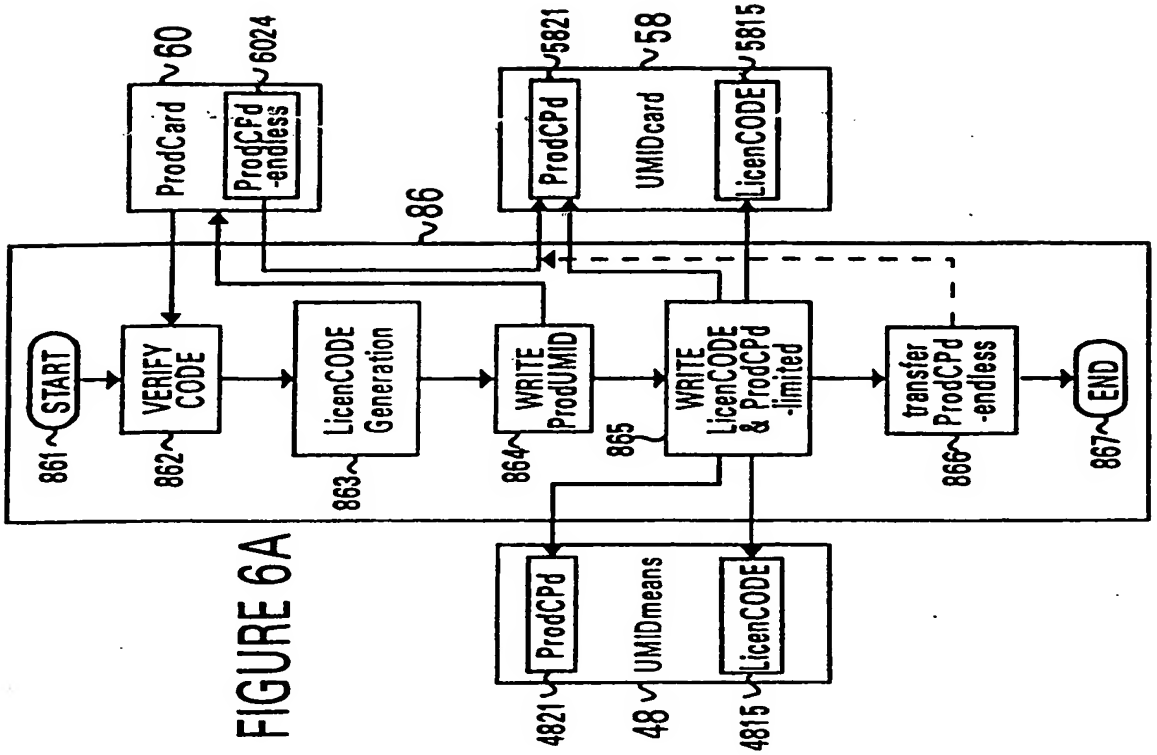


FIGURE 6A

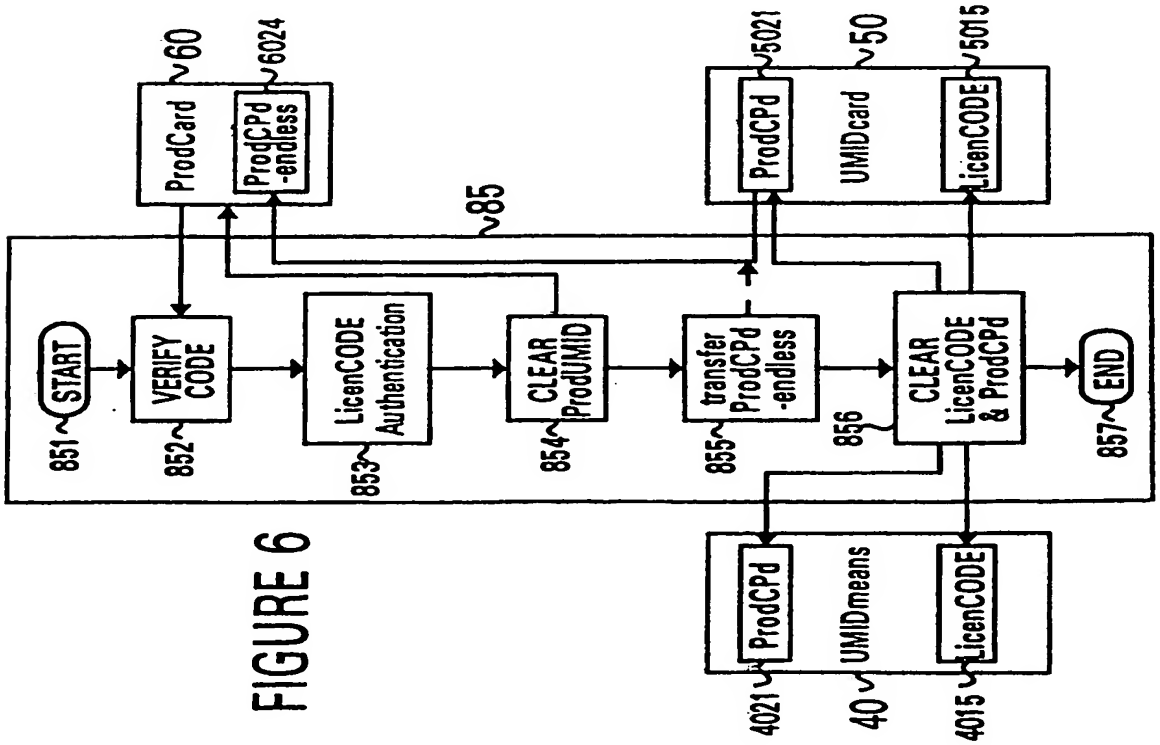


FIGURE 6

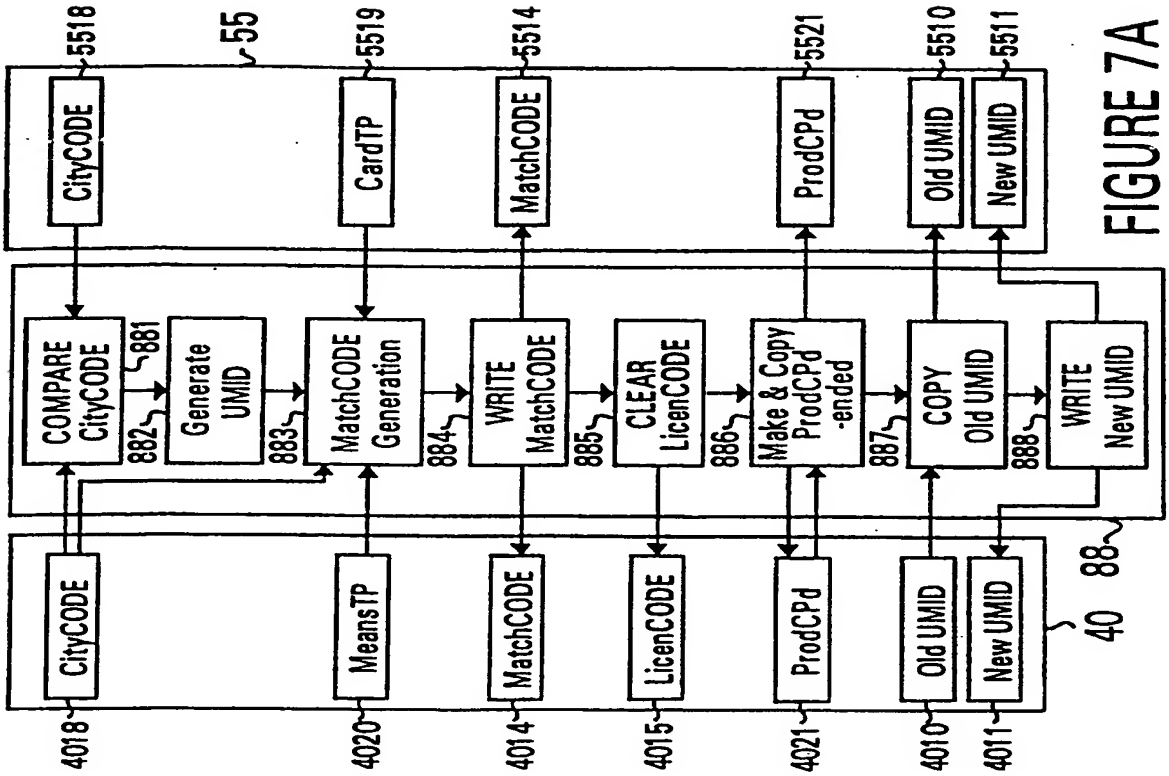


FIGURE 7A

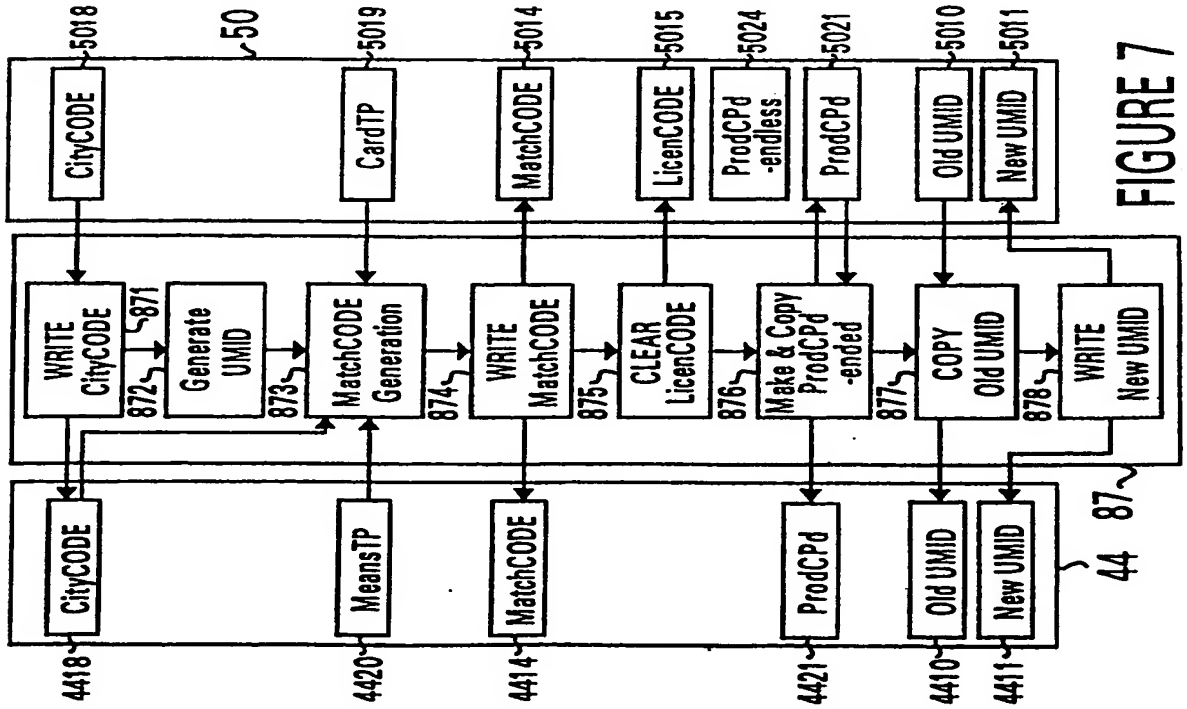


FIGURE 7

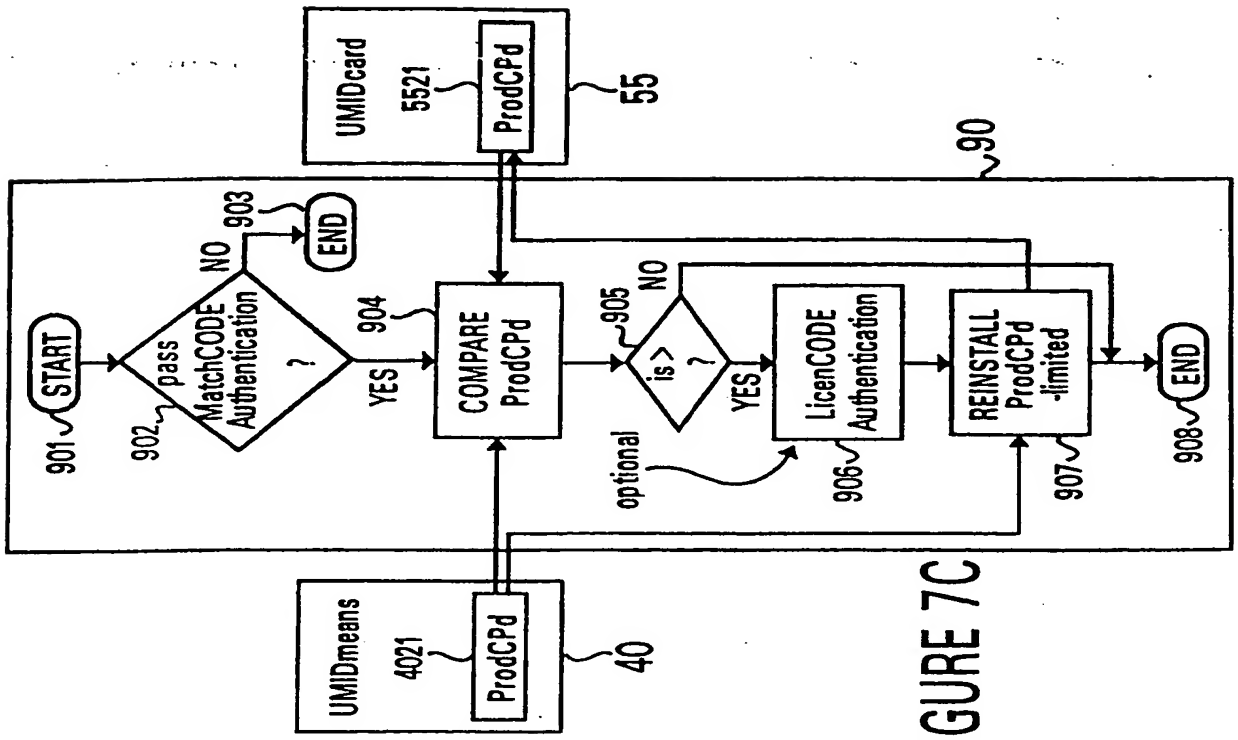


FIGURE 7C

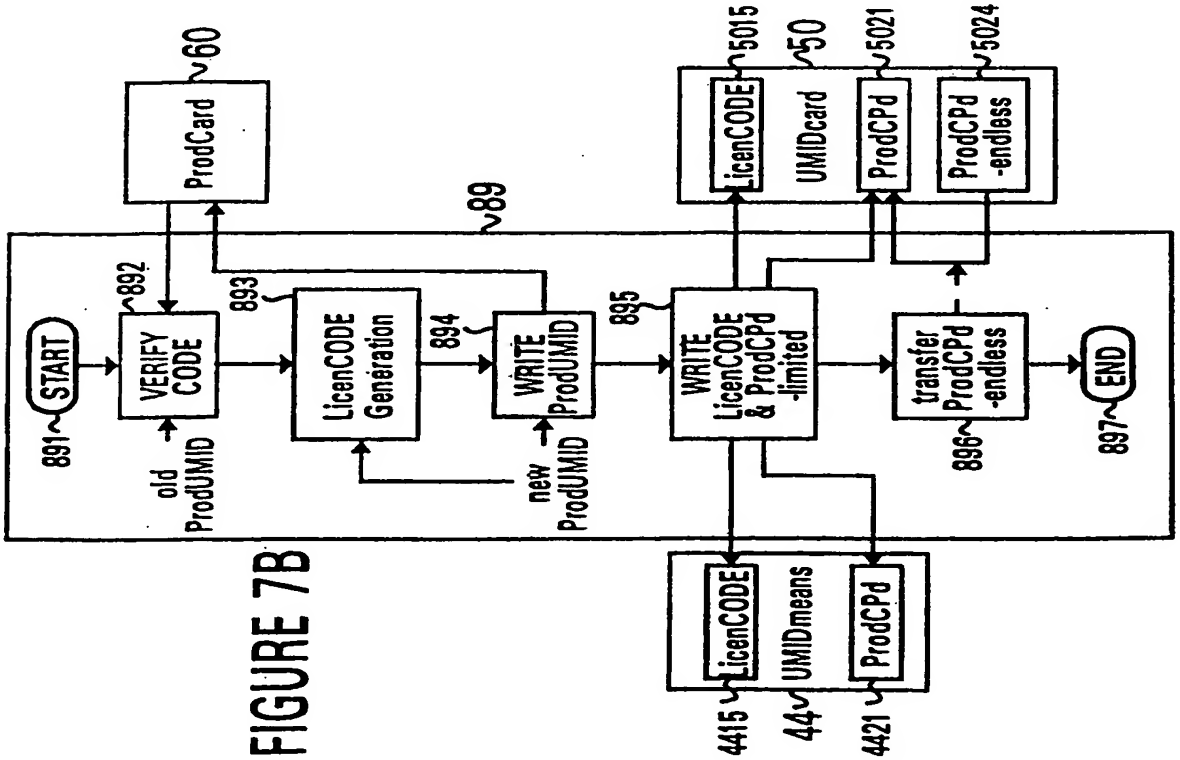


FIGURE 7B

SDOCID: <WO_____9903031A1_I_>

FIGURE 8A

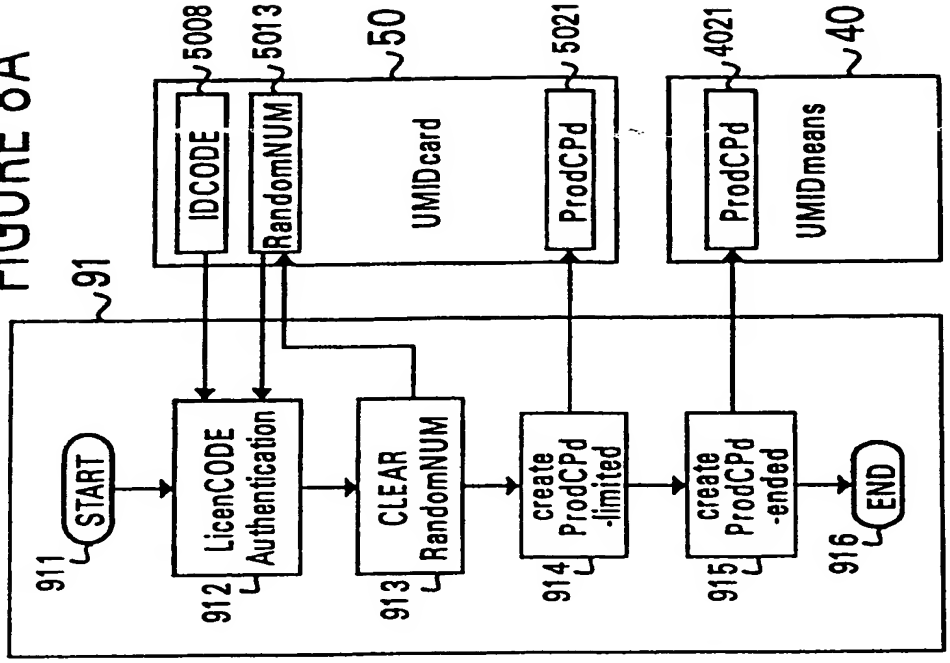


FIGURE 8

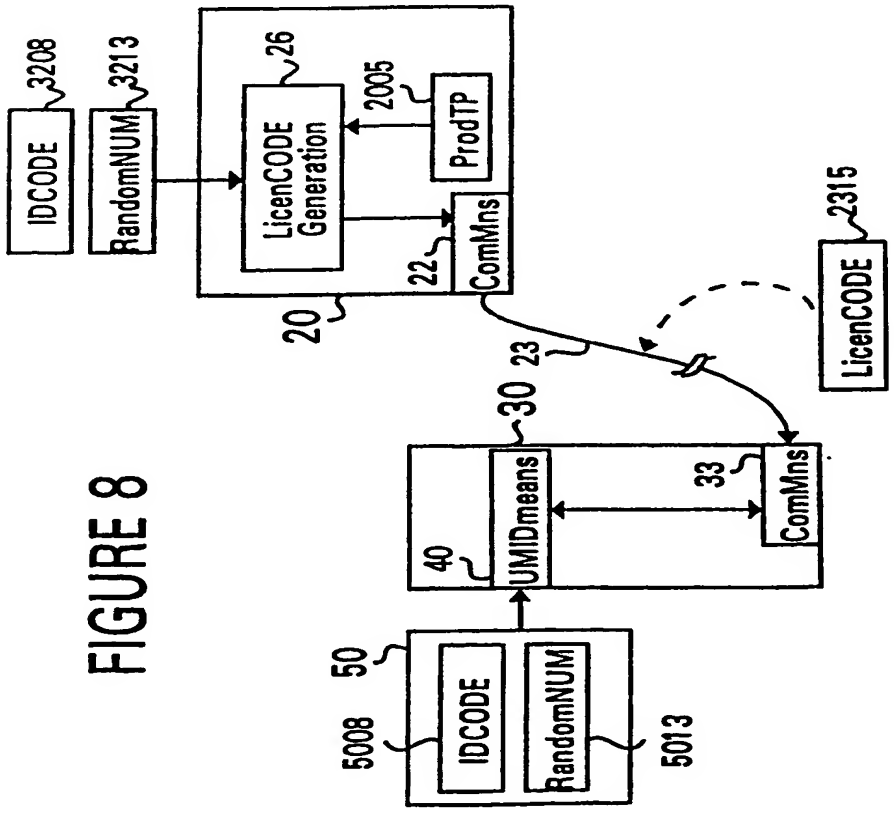


FIGURE 10

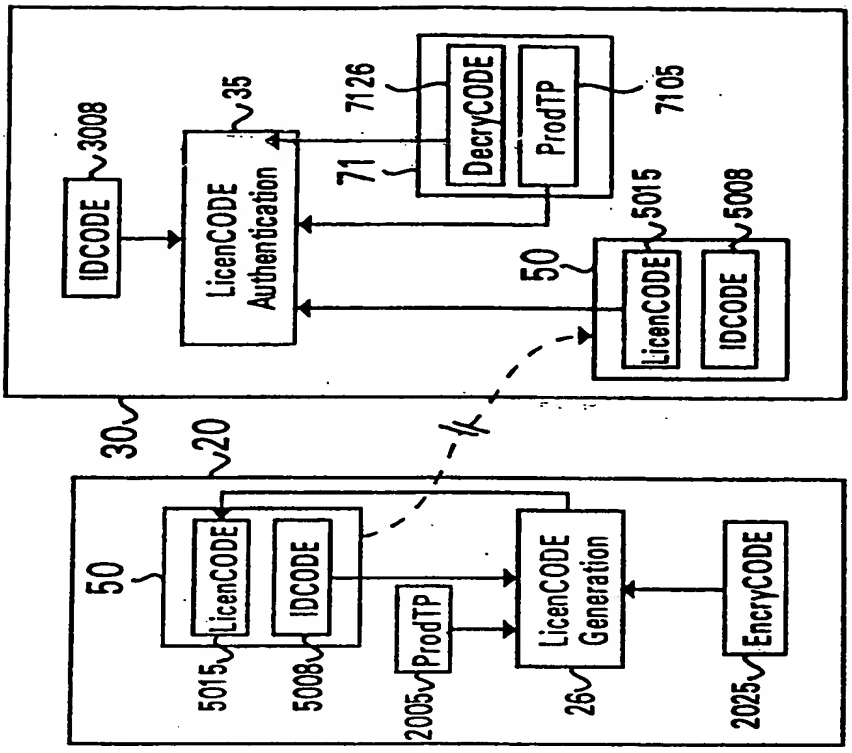
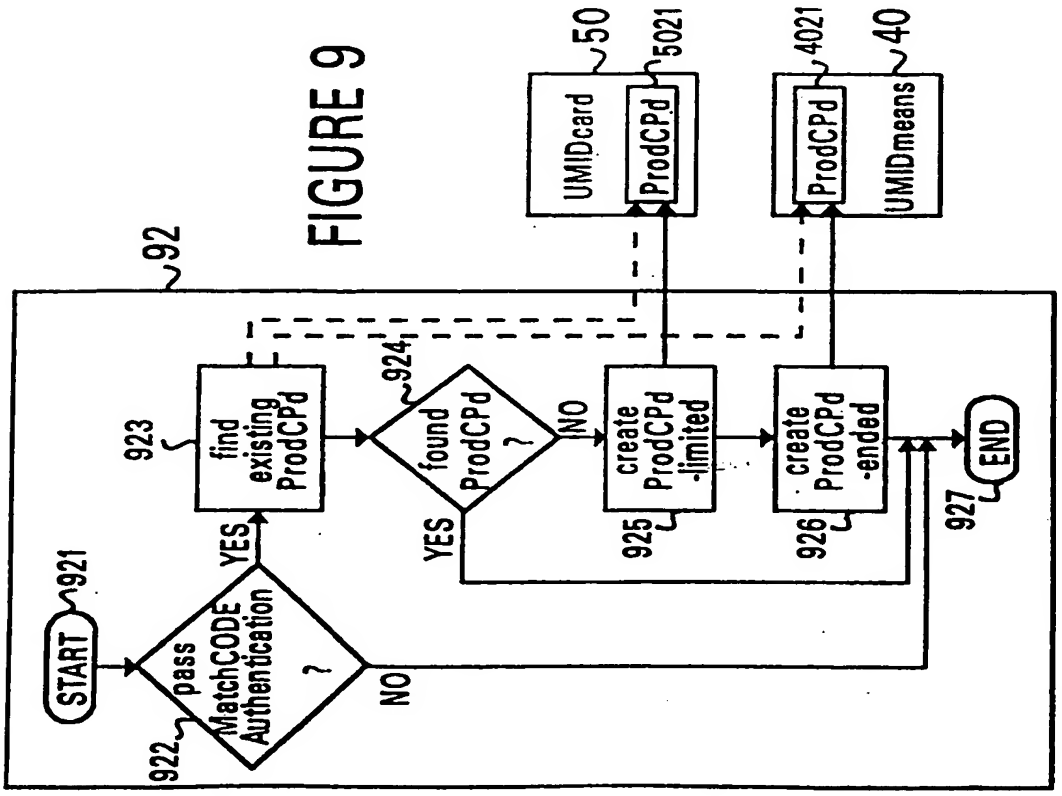


FIGURE 9



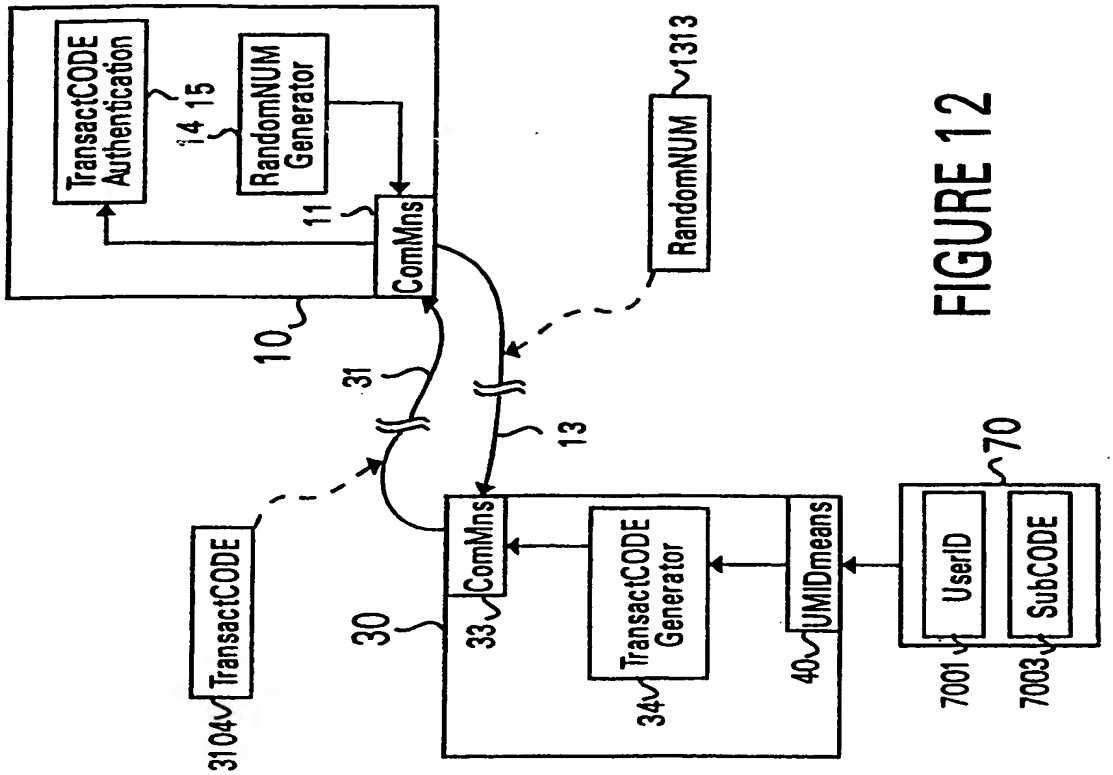


FIGURE 12

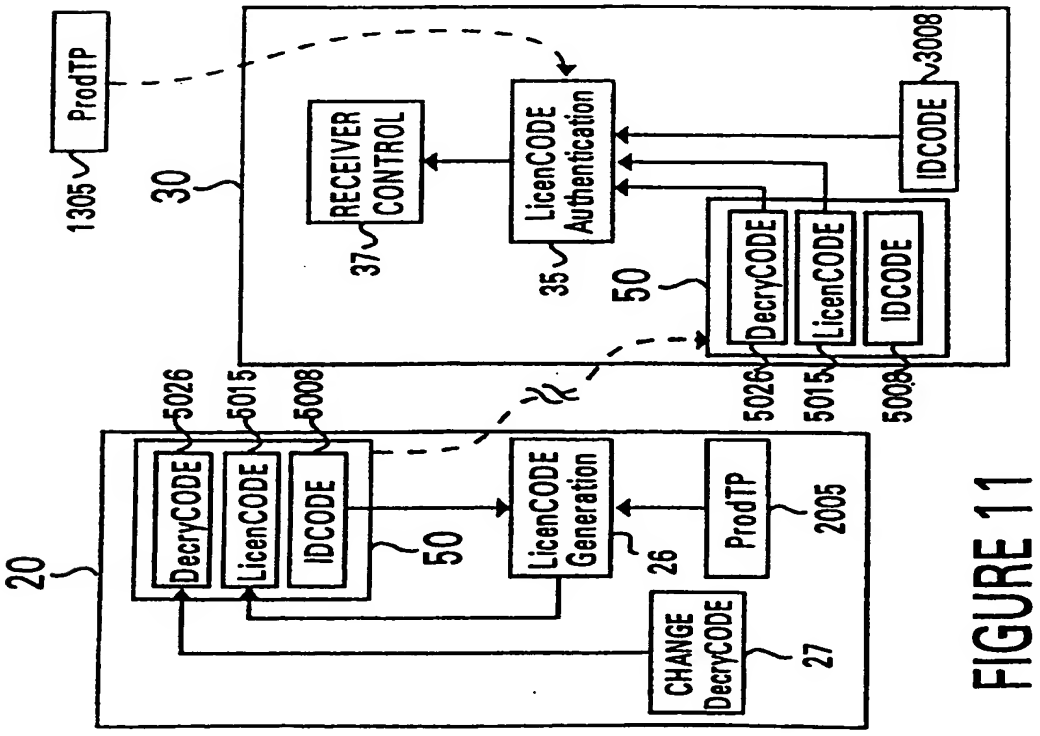


FIGURE 11

FIGURE 12B

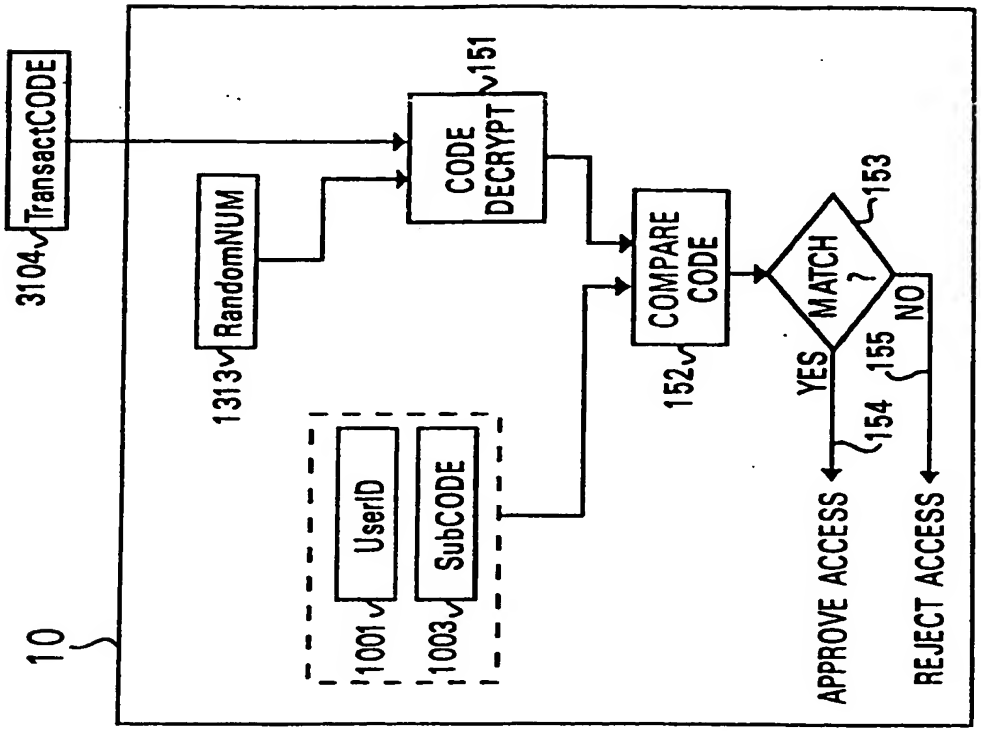
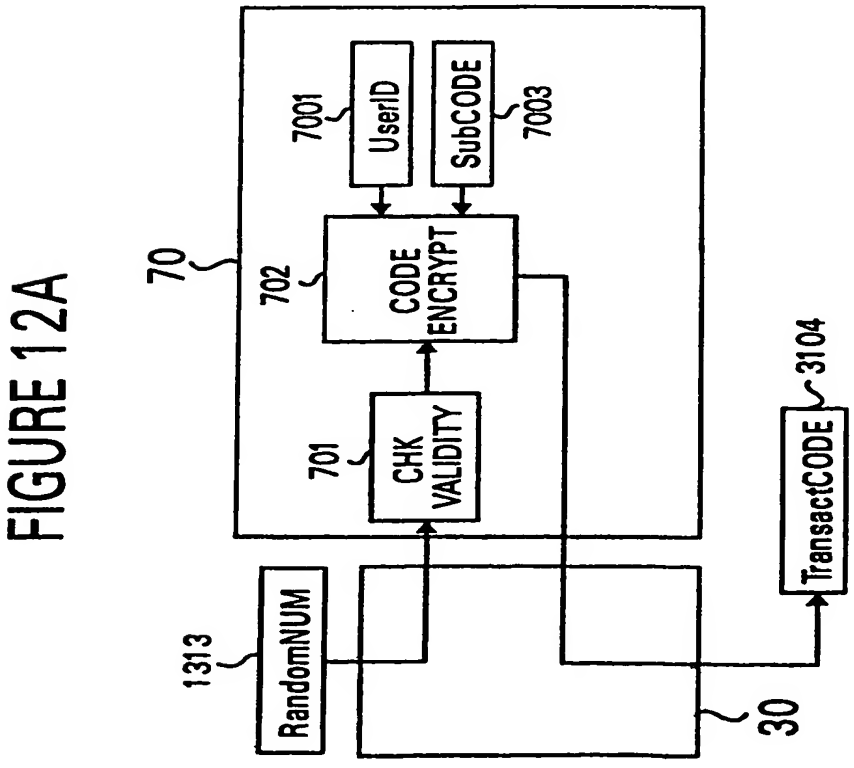


FIGURE 12A



INTERNATIONAL SEARCH REPORT

Inter ..ional application No.
PCT/SG 98/00053

A. CLASSIFICATION OF SUBJECT MATTER

IPC[6]: G 06 F 1/00, 12/14; H 04 L 9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC[6]: G 06 F, H 04 L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 97/03 398 A1 (SIGBJORNSEN) 30 January 1997 (30.01.97), abstract; page 1, line 4 - page 6, line 8; page 6, line 31 - page 8, line 10; fig. 1-6.	1,10,11,14, 21-23,25
A	DE 44 19 115 A1 (DÖLKER) 20 October 1994 (20.10.94), abstract; column 1, line 3 - column 3, line 35; fig.	1,10,14,21, 22,25
A	EP 0 302 710 A2 (INTERNATIONAL BUSINESS MACHINES) 08 February 1989 (08.02.89), abstract; page 2, line 3 - page 5, line 24; fig. 1,2 (cited in the application).	1,10,11,14, 21-23,25
A	US 5 440 631 A (AKIYAMA et al.) 08 August 1995 (08.08.95), abstract; column 1, line 8 - column 2, line 50; column 5, line 64 - column 10, line 63; fig. 1-4.	1,10,11,14, 21-23,25
A	US 5 337 357 A (CHOU et al.) 09 August 1994 (09.08.94), abstract; column 1, line 11 - column 4, line 37; fig.	1,11,14,23,25

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 October 1998 (20.10.98)	04 November 1998 (04.11.98)

Name and mailing address of the ISA/ AT	Authorized officer
Austrian Patent Office Kohlmarkt 8-10; A-1014 Vienna	Hajos
Facsimile No. 1/53424/535	Telephone No. 1/53424/410

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Inter .ional application No.
PCT/SG 98/00053

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 392 351 A (HASEBE et al.) 21 February 1995 (21.02.95), column 1, line 6 - column 2, line 5; column 3, line 9 - column 5, line 16; fig. 1,2.	1,11,14,23,25

Form PCT/ISA/210 (continuation of second sheet) (July 1998)

OCID: <WO_____9903031A1_I_>

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intc ..ional application No.
PCT/SG 98/00053

Im Recherchenbericht angeführtes Patentdokument Patent document cited in search report Document de brevet cité dans le rapport de recherche	Datum der Veröffentlichung Publication date Date de publication	Mitglied(er) der Patentfamilie Patent family member(s) Membre(s) de la famille de brevets	Datum der Veröffentlichung Publication date Date de publication
WO A1 9703398	30-01-97	AU A1 65357/94 EP A1 855052 NO A0 952795 NO A 952795 NO B1 302388 PL A1 324525	13-02-97 29-07-98 13-07-95 14-01-97 23-02-98 08-06-98
DE A1 4419115	20-10-94	keine - none - rien	
EP A2 302710	08-02-89	CA A1 1292791 EP A3 302710 JP A2 1044542 US A 4866769	03-12-91 10-01-90 16-02-89 12-09-89
US A 5440631	08-08-95	JP A2 5298085 US A 5737413 JP A2 6095871	12-11-93 07-04-98 08-04-94
US A 5337357	09-08-94	CA AA 2120816 EP A2 636962	18-12-94 01-02-95
US A 5392351	21-02-95	EP A2 561685 EP A3 561685 JP A2 5257816 US A 5555304 US A 5796824	22-09-93 22-12-93 08-10-93 10-09-96 18-08-98